# COLLUSION RESISTANT MULTIMEDIA FINGERPRINTS

**HEMED HASHIL SAID**
**Roll. 213CS2502**
Master of Technology
In
Computer Science Engineering
(Information Security)

*Under the guidance of*
**Dr. RUCHIRA NASKAR**


**Department of Computer Science and Engineering**
**National Institute of Technology, Rourkela**
**Rourkela – 769008, India**

# COLLUSION RESISTANT MULTIMEDIA FINGERPRINTS

*Thesis submitted in*

*June 2015*

*to the department of*

***Computer Science and Engineering***

*of*

***National Institute of Technology, Rourkela***

*in partial fulfillment of the requirements*

*for the degree of*

***Master of Technology***

*by*

***HEMED HASHIL SAID***

***(Roll. 213CS2502)***

*under the supervision of*

***Dr. RUCHIRA NASKAR***


**Department of Computer Science and Engineering**

**National Institute of Technology, Rourkela**

**Rourkela – 769008, India**

Computer Science and Engineering
**National Institute of Technology Rourkela**
Rourkela-769008, India. www.nitrkl.ac.in

June 1, 2015

# Certificate

This is to certify that the thesis entitled **"Collusion Resistant Multimedia Fingerprints"** submitted by **Hemed Hashil Said**, in partial fulfillment of the requirements for the award of Master of Technology in the Department of Computer Science Engineering, with specialization in Information Security at **National Institute of Technology - Rourkela** is a genuine thesis carried out by him under my guidance and supervision. To the best of my knowledge, the material personified in the thesis has not been submitted to any other University, College or Institute for the award of any Degree or Diploma.

Date:

**Dr. Ruchira Naskar**
Assistant Professor
Department of CSE
***Thesis Supervisor***

# Acknowledgment

I would like to spread my gratitude and my sincere thanks to my supervisor Dr. Ruchira Naskar, Asst. Professor, Department of Computer Science Engineering for her continuous inspiration and support during the course of my thesis in last one year. I am obliged to her for having helped me outline the problem and providing visions towards the solution.

I extend my gratitude to the Head of the Department of Computer Science Engineering for his priceless suggestions and continuous inspiration all through the thesis work.

I will be failing in my duty if I do not mention all Professors and administrative staff of this department for their help.

Last but not the least this thesis would have been difficult without the continuous ethical support from my family members, my lovely wife, my best friends. I would like to thank them all.

***Hemed Hashil Said***

***(Information Security)***

# Abstract

Multimedia fingerprint is a technique for investigating the distribution of multimedia content (such as audio, image, video, etc.) and securing them from unapproved reallocation. Unique approval information is inserted or embedded into each scattered copies of multimedia data, with each multimedia content fingerprint allocated to a proposed recipient. Collusion attack is a well known attack on multimedia fingerprinting, by which attackers combine multiple copies of the same multimedia content, but with dissimilar fingerprints. Therefore collusion poses a real challenge to protect multimedia information.

This thesis surveys the state of the art collusion resistant digital fingerprinting algorithms and presents an analysis of these fingerprinting techniques. We investigate elementary linear and nonlinear collusions on self-determining fingerprints and analyze severities. In this thesis, we developed a web application implementing collusion resistant fingerprint algorithms and study their performance under collusion attacks.

# Contents

# List of Figures

# Chapter 1

# Introduction

Media and broadcast industries are highly dependent on the integrity and credibility of multimedia data. In such industries it is important to protect multimedia data against illegal distribution and to ensure that data is distributed only authorized recipients. To solve this problem we need a technology to recognize and find individuals who contributed in illegal distribution of multimedia data. Multimedia fingerprinting is a method of generating that unique identification, named digital fingerprints, which are embedded into several copies of the similar multimedia prior to distribution. Digital fingerprints are used to investigate the such illegal recipients. For efficient protection of multimedia, it is required that the fingerprints strong linked with the multimedia data.

Fingerprinting is a strategy that prevents unlawful distribution of media information. A collusion is a contract between two or more parties, occasionally unlawful to defrauding others of their lawful rights by defrauding an unfair for unlawful distribution. Fingerprinting techniques for collusion resistant attack are categories into two main groups: Orthogonal and coded.

There are numerous categories of collusion attacks on fingerprinting techniques. One way applied is to match the media components and average them, this known as the linear collusion attack. Second one is a copy and paste collusion, which has recipients extracting parts from their individual legal copies and combine them

to create fresh copy. Nonlinear operations are an additional collusion which can work by using the median or a maximum of a number of duplicates of the same multimedia data. Our motivation is a comparison of linear, nonlinear and average collusion attacks for fingerprinting algorithms.

It is very easy for people to combine numerous copies of the same multimedia to carry out collusion attack. These assaults conventional called collusion assaults, offer a charge actual process for eliminating and recognizing fingerprint and present substantial hazard to fingerprinted multimedia. Aimed at an inappropriately fingerprint designed, it is likely to shape a minor organization of colluders and adequately weaken separately colluders perceiving fingerprints to make a crisp release of the substance with no discoverable investigates. Hence, designing fingerprints that battle collusion attacks and determine the existence of colluders, it is very essential.

To make fingerprints Collusion resistant, the designer should consider several issues in a fingerprinting system like detection mechanism, strength of the fingerprint, and computational cost. Additionally, whether detection should be blind or non-blind whether designer selected suitable storage resources, computational resources and other suitable performance criteria are given by Catch One, Catch Many, Capture All colluders. In this thesis, we analyze a key strategy for multimedia collusion resistant fingerprinting and compare several existing fingerprinting methods.

Before examining collusion resistance performance of an accurate fingerprinting application, It is necessary to answer three fundamental questions: Firstly, how to measure the collusion resistance of a fingerprinting application? secondly, detailed fingerprinting application (there are two main issues: the designing of fingerprint, and scheme of detection). Finally to explain application necessities for overcoming collusion attacks.

## 1.1 Criteria for Designing Multimedia Fingerprinting

Nevertheless one group of collusion is worked out, the general aim of the fingerprinting is to protect and arrest the opponents and break the propagation of untrue content of multimedia. Though, several concerns get up below this situation, and the fingerprinting designed should be suitable criteria to perform better performance. Probable aims for planning fingerprinting as follows:

Firstly criteria is catching one colluder, The aim of designing the fingerprinting to increase the opportunity of catching at minimum one colluder, whereas looking to reduce the likelihood of falsely critical a guiltless recipient, the established of presentation criteria contains of the chance of a false desirable and the chance of a false undesirable. Since the receiver's side, a recognition method has failed. The receiver fails to recognize slightly no one colluders or the receiver falsely shows that a guiltless recipient is a colluder.

Secondly criteria is catching many, this situation many colluders to be possible captured, however, possibly at a cost of critical extra guiltless recipients, the criteria, presentation contains of the estimated division of colluders that positively arrested, and the estimated division of guiltless recipients that falsely located in distrust [23].

Thirdly criteria is capturing all, the fingerprinting are intended design situation to exploit the chance of arresting all colluders, even though continuing an acceptable volume of guiltless recipient's presence falsely defendant. This situation gets up once the honesty of the information recipients is of such excessive anxiety that all recipients participated in the information leakage need to be recognized. This criteria contains of traditional of presentation computing the chance of arresting all colluders, and a competence rate, which terms the estimated volume of falsely blamed guiltless per colluder [23].

## 1.2 Designing Collusion Resistant Fingerprints Considerations

- The fingerprinting the designer should reflect how fingerprinting recognition will take place.
- The appropriate strength aimed at the fingerprinting designed.
- In what way fingerprinting computationally capable the colluder recognition patterns necessity to be.
- The consideration of designer should be involved original multimedia in the recognition stage of the fingerprinting system (non-blind detection) or should not be existing in the discovery stage of the fingerprinting system (blind detection).
  - Non-blind recognition is the method of discovering or identifying the embedded multimedia with the assistance of original multimedia, Non-blind fingerprint detection delivers high assurance in detection. Non-blind fingerprint detection involves a process of knowing the multimedia from a database that may need significant storage means.
  - Blind recognition is the method of discovering or identifying the embedded multimedia without the information of the original multimedia. The blind discovery allows intended for spread detection situations file does not need huge storage memory or significant calculating costs related to multimedia recording.

## 1.3 Kinds of Collusion Attacks

### 1.3.1 Linear Collusion Attacks

Linear collusion attack is the greatest realistic collusion attacks that can work alongside multimedia fingerprints. Supposed various severally fingerprinted duplicates of the same multimedia content, the linearly colluders association together all the duplicates to create a colluded duplicate. In linear collusion attack a K-colluder, the fingerprinted indicators xi are joint giving to$\sum_{i=1}^{k}\lambda$ixi, where the weights $\lambda$i satisfy $\sum_{i=1}^{k}\lambda$i=1 to continue the average strength of the multimedia signal as original. Through fingerprinting orthogonal, intended to colluder i that allocated the load $\lambda$i, the strength of this fingerprint is minimized by an issue of ($\lambda$i)square . After $\lambda$i is minor, the investigation of colluder i's fingerprint is lack of physical strength and colluder i is fewer rare elect trapped by the receiver.

Many collusion attacks, meanwhile not at all colluder could comparable to the possessive additional of a danger than another colluder, regularly they decide to allocate the hazard of presence identified consistently amongst all members then spread over reasonable collusion. The best way to accomplish objectivity of collusion is to average fingerprinted information's per an identical weightiness for individually recipient and use $\lambda$i = 1/K for altogether i. Figure 1.1 displays three colluders, making collusion by averaging where by altogether three fingerprints (Alex, John, and Jacklyn) are averaged with the same weight 1/3.

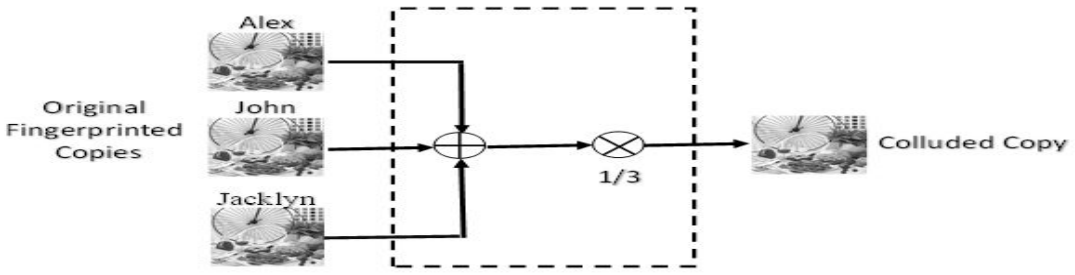


Figure 1.1: Averaging Collusion Attacks.

### 1.3.2 Copy and Paste Attacks

One more kind of collusion, denoted is known as copy and paste collusion, includes recipients cutting parts of individually of multimedia components and pasting those parts organized to create a fresh version. For instance, of the copy and paste attack by two colluders, Alex and Jacklyn. The colluded version duplicate is generating half of his overall fingerprint energy that displays in Figure 1.2. So, the outcome on the fingerprint lacking of physical strength and the influence on the chance of presenting identified, we can reflect copy and paste collusion similar to average built collusion once regarding inserting spread spectrum. Through taking the half left of Alex's fingerprinted part and copying the half right of Jacklyn's part. Where by the fingerprint is distributed all over the whole host signal by embedding spread spectrum technique and identified over around form of correlation handling, the copy paste collusion has the result as similar to averaging collusion. In all situations, the lacking of physical strength of fingerprint of each paying fingerprint is lack of physical strength by a factor equivalent to the quantity of duplicates included into collusion "if Alex donates half of his trials copy and paste attack, the strength for Alex's fingerprinted in the colluded duplicate is involved".

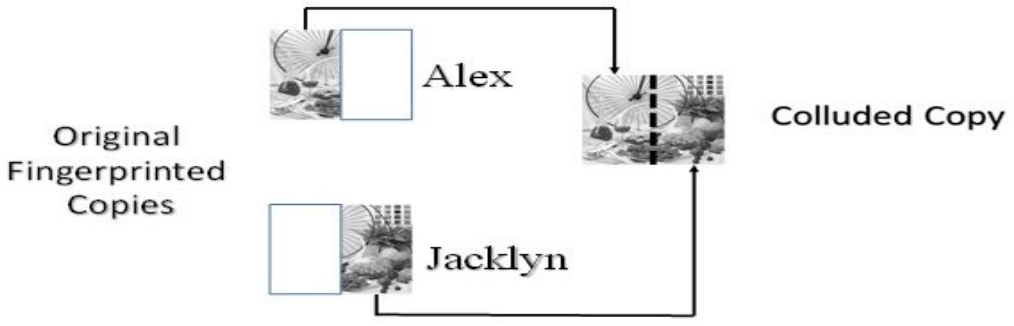


Figure 1.2: Copy and Paste Collusion Attacks.

### 1.3.3 Collusion Attacks (Nonlinear)

Linear Linear collusion using averaging is an easy and operative method for a combination of recipients to reduce inserted fingerprints. However Averaging is form of collusion obtainable of a combination of opponents, but for individualist element of the signal of multimedia, the colluders may result in rate among the maximum and minimum equivalent rate, and consume high assurance that the fake quality they receive will be of the variety of the just noticeable different into individually fingerprinted duplicate is anticipated to expend high perceptual excellence. Nonlinear significant of collusion attacks is founded on operations by attractive the minimum, maximum, and median of matching elements of the fingerprinted colluders duplicates. Figure 1.3 displays various kinds of nonlinear properties into three colluders, Alex, John, and Jacklyn. For every pixel at the nth column and the mth section in the image, gathered that having the 42, 43, and 46 qualities in the three duplicates coordinating to the three colluders. Subsequent to making the conspired copy, for the pixel at column n and segment m, the colluders may have the least of the three qualities, which gives 42 and they might likewise utilize the most maximum or the medium of the coordinating pixels in the three duplicates, which are 46 and 43, separately. Through collusion, the aggressors might likewise affiliation these rudimentary methodology make a duplicate colluded. Planned for utilizing pixel at section m and column n in the colluded duplicate, then colluders may take the average of the maximum and the minimum, which is 44. The colluders replication this methodology for every pixel in the image and produce the colluded copy.

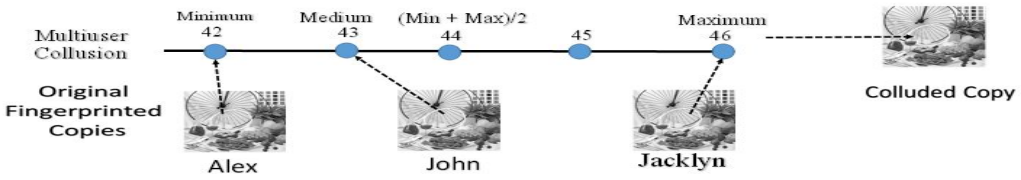


Figure 1.3: Nonlinear Collusion Attacks.

## 1.4 Elementary Embedding Methods

The data embedding process is usually starts by an original digital media (D0), host media is also identified as the implanting component inserts or integrated into multimedia data (x), which is mentioned as embedded information, to achieve the covered media (D1). The embedding is completed that D1 is same matching to D0. The difference between D1 and D0 is the distortion presented by the inserting procedure. This scenario, the embedded information is a group of bits, which may originate from an encrypted side that is bits series from a design the system depending on. The inserted information x will be removed from the covered media D1 by a detector, frequently next D1 has been made by different treating and assaults. The process of decoder is mentioned as a test signal (D2), and decoding information D2 is represented by x. The difference among D2 and D1 is named noise. The applications as ownership defense, access control, and fingerprinting, correct extracting of covered data from distorted test media is favored. The embedding of bits in host media is elementary to each hiding data application. Nearly all inserting methods are two general kinds. We explained those methods as follows.

In the first kind inserting, the multimedia information, maybe encrypted, controlled, and mounted, is inserted into the host media, the addition can be performed in a particular structure. To insert bit x, the several among the covered signal D1 and the original host component D0 is a function of x, that is, D1-D0 = f (x). While it is probable to identify b straight from D1, the information of D0 supports improved recognition performance. Fingerprinting additive spread spectrum is for instance of first embedded Kind, as displayed in Figure 1.4

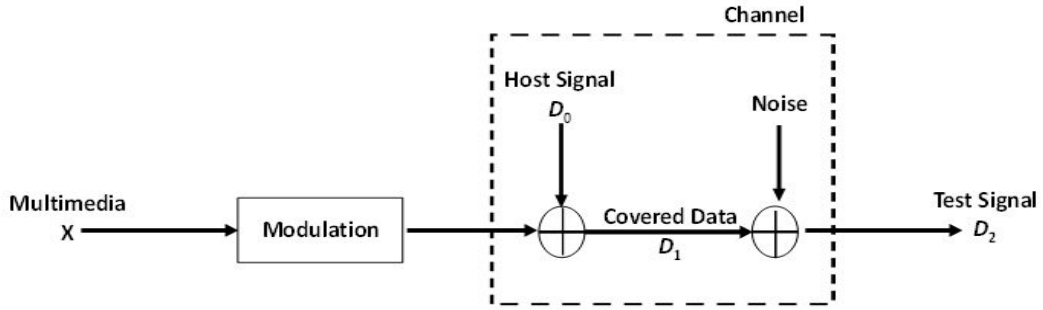


Figure 1.4: Embedding Process for Modulation.

Another second embedding kind, the component space is divided into subsections, individually one is mapped through a function g(.) to the fixed of values engaged by the multimedia information's, The marked value D1 is then chosen from the subsection that maps to x, hence the association between x = g(D1) is regulate enforced. Perceptual distortion is minimized, D1 must be as near to D0 as probable. For instant odd-even is embedding, therefore nearest even number is applied as D1 to insert a "0", and a nearby odd number is applied to insert a "1". The inserted bit has been decoded just by testing the odd even parity that does not need the information of original D0. These may be other limitations enforced on D1 for robustness concerns. As displayed in Figure 1.5.

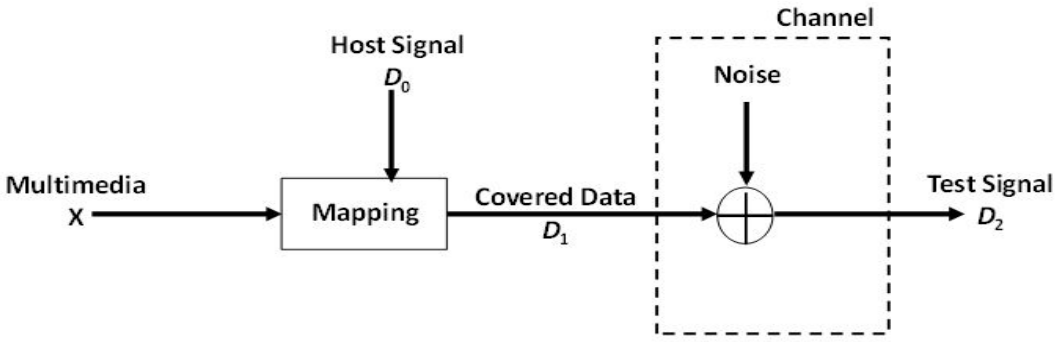


Figure 1.5: Embedding Process for Mapping.

## 1.5 Collusions Resistant Fingerprinting Techniques

There are two primary classifications for collusion averaging assault resistant fingerprinting methods. The principal strategy is orthogonal fingerprinting procedures where every recipient is appointed a spread spectrum succession that is commonly orthogonal to one another as a fingerprint. Another technique is known as coded procedures that utilization collusion resistant fingerprint.

### 1.5.1 Orthogonal Technique

The orthogonal is a direct technique for digital fingerprinting. In this technique, N orthogonal signs are utilized to suit N beneficiaries, which is a commonly orthogonal sign is dispensed to every beneficiary as a fingerprint to choose the multimedia proprietor or to follow colluders who arranged unlawful duplicates, the same number of connection as the quantity of beneficiaries is obliged so that the recognition discovery is high. In extra disadvantage is that when the quantity of multimedia included in the averaging assault expands, the quality of orthogonal signals is weakened deservedly so that the detector can't effectively follow colluders. Gathered that relationship is utilized as a recognition measurements and M beneficiaries join to the coalition to make illicit duplicate V. The sign of every beneficiary is orthogonal which relationship qualities will be decreased in conversely corresponding to the quantity of colluders M. This demonstrates a disadvantage of indicator when orthogonal signals are founding the middle value of together, and we can think about when the high number of beneficiaries joins to get ready illicit duplicates, orthogonal regulation plan will neglect to recover colluders effectively. We saw that the multifaceted nature of disclosure could be a sympathy toward fingerprints of orthogonal. Other issue through orthogonal fingerprinting climbs once investigative the vitality decline of the fingerprint segments through collusion. Under collusion averaging the decrease is important and on the same direction as the measure of

colluders.

Additionally, the amount of recipient's quantity that may be sustained via an orthogonal fingerprinting scheme, is equivalent to measurement of the fingerprint. In numerous multimedia distribution uses, this limits the number of customers that multimedia can be distributed to them. The orthogonality permits fingerprints to the large amount. The straightforwardness of encrypting and embedding orthogonal fingerprints makes them beautiful to systems involving a minor set of recipients.

### 1.5.2 Coded Technique

The coded strategy was defined to possessive numerous beneficiaries than that of the orthogonal technique with the same measure of signs. Trappe proposed an agent coded technique [2]. The fingerprint signal for the jth beneficiary, wj, is made by a linear combination of an entire of multimedia signal ui. The binary fingerprint codes inferred to serve to beneficiaries averaging resistance. Averaging of up to codes results in an exceptional code which can perceive all codes related with the averaging. A fingerprint signal for the one beneficiary is made out of code bits and orthogonal sign as demonstrated as follows. wj=$\sum_{i=1}^{M}$bij.ui

Where bij are 1, that is duplicated by ui relying upon an i-th bit of j-th beneficiary codes then ui are orthogonal signs utilized for i-th bit area. In identifier side, bij are acquired by the relationship between wj and ui with a limit esteem. In which several fingerprint codes are averaged, the distinguished code is a touch insightful intelligent of that fingerprint codes. For looking at bit areas where the quality is 1 in averaged code with a code book, the detector can disclosure out that codes are included in the association.

With a specific end goal to plan these fingerprints so they have well against collusion belonging. We must build these fingerprints by utilizing code balance [7]. By which to add to the codes so that the connections are deliberately acclimated into the few fingerprints to allow the right agreement assault ID included in an assault. Regularly, the codes are binary codes, however late endeavors

have investigated genuine esteemed code developments [28]. In Coded fingerprint to neutralize the energy decrease by reason of collusion, to present association amongst the fingerprints, once colluders association their fingerprints definitely interrelated modules of the fingerprints do not familiarity as important reduction of vitality. Another merit of using the code scheme is may be able to signify extra v recipients, when using v orthogonal source signals. Also, fingerprint code modulation designing is the strategy to create the relationship between several fingerprints to permit perfection identification of the collusion that is performed in contributing fingerprints.

## 1.6 Chapter Organization

This thesis addresses the issues regarding collusion resistant multimedia fingerprints. The work included in this thesis aims to implement existed algorithms proposed against different collusion attacks, by implementing coded fingerprinting algorithms using additive spread-spectrum embedded technique. Two fingerprinted algorithms have been discussed in this chapter. The first one is orthogonal fingerprinting. The second one is coded fingerprinting. The chapters of this thesis are organized as; the literature review on various scholar views about collusion resistant is presented in Chapter 2. Theoretical Analysis on fingerprint and collusion attacks has been discussed in Chapter 3. The implementation part has been discussed in Chapter 4. At last Chapter 5 introduces the closing comment, with extension for further research work.

# Chapter 2

# Literature Review

This chapter provides the review of the issues that have been explored and studied both theoretically and empirically in the existing literature made by other scholars and academicians on collusion resistant multimedia fingerprints. This some Literature review covers different knowledge of various authors about this thesis.

Digital fingerprints are one of a kind names embedded in various duplicates of the same substance before spreading. Each digital fingerprint is allocated to a planned beneficiary, and can be utilized to follow the offenders who utilize their substance for unintended purposes. Assaults mounted by different recipients, known as collusion assaults, give a savvy technique for weakening the distinguishing fingerprint from each colluder. Accordingly collusion represents a genuine test to ensure the computerized media information and implement utilization approaches as clarified by Wade Trappe el at [23]. The arrangement assault from a gathering of illicit clients (colluders), consolidating different duplicates with the same digital multimedia, yet diverse fingerprints to attempt to uproot the inserted fingerprints or casing pure recipients. On the off chance that an unlawful duplicate shows up, the recipient data can be separated to help follow or recognize unapproved recipients [11].

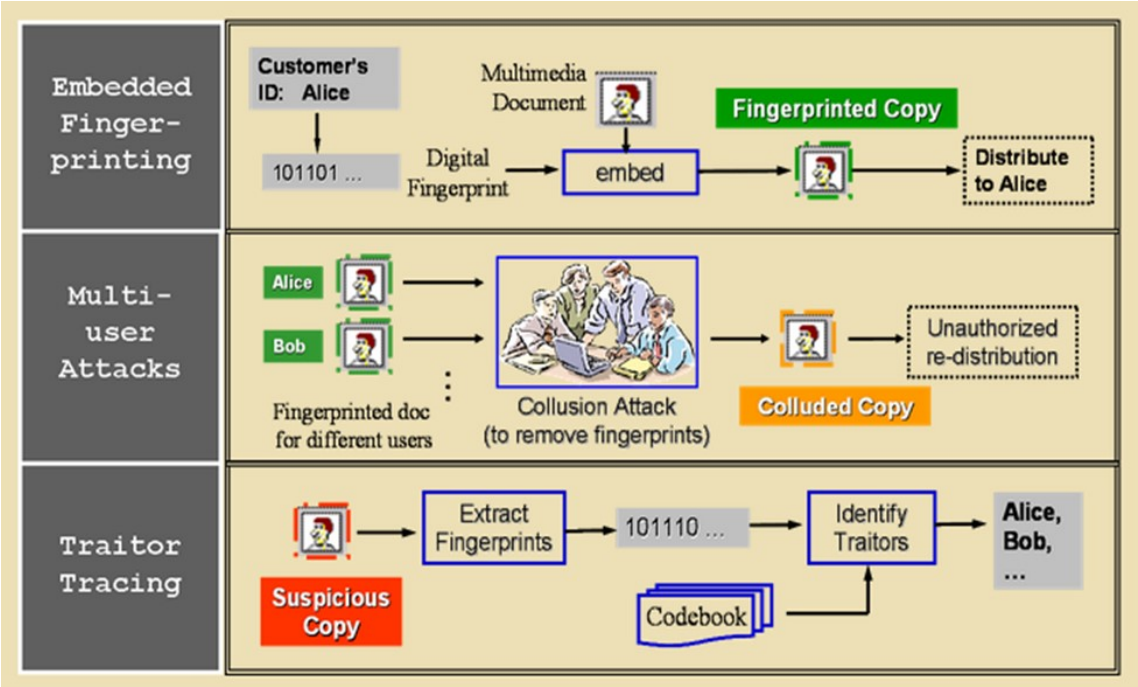


Figure 2.1: Using Embedded Fingerprinting for Tracing [11].

Wang et al. [28] have suggested that traitors are more prone to collude with beneficiaries who offer regular highlights, for example, social circumstances or geographic region. In this theory, a progressive fingerprinting method taking into account added substance spread spectrum has been recommended. Utilizing proposed strategy, beneficiary are allocated to gatherings, and the fingerprint is produced using the beneficiary ID and its gathering ID. At the discovery stage, to begin with, the gathering of colluders is perceived and afterward the beneficiaries who have a place with that gathering are perceived. This minimizes the computational cost alongside the likelihood of false-positive identification.

Shuhui Hou and D. Kundur et al. proposed significant applications and configuration necessities computerized watermarking has been sought various applications identified with interactive media content assurance and security. These incorporate proprietorship insurance, verification or altering identification, computerized fingerprinting, duplicate control and access control etc. Computerized

fingerprinting is one use of digital watermarking. Fingerprint installing or discovery serves to stamp each legal duplicate particularly with the inserted fingerprints and follow the cause of an unlawfully utilized duplicate with the identified fingerprints. Computerized watermarking and computerized fingerprinting have their own configuration prerequisites as far as the subtlety, the power, and the inserting limit measured by what number of bits are inserted. Computerized fingerprinting comprise of insert multimedia recipient's data, suggestion multimedia recipient re-disperses multimedia unlawfully and a wide range of fingerprinted multimedia [12, 5].

On the other hand, computerized fingerprinting was at first used to face the unlawful dispersion of interactive multimedia, for example, images [15], sound [6], and video [16], however, this technique has been additionally used to guard computerized documents [20], convincing beneficiaries, not to supply privateer duplicates and recognizing the beneficiaries. In this circumstance, fingerprinting will be utilized as a trade for computerized fingerprinting and fingerprint will be utilized to signify to the extraordinary ID of every beneficiary. For the value of fingerprinting strategies, it is must fulfill two principle properties; Perceptual straightforwardness; the original multimedia and its fingerprinted duplicate must be indistinguishable to the beneficiary discernment. This is measured utilizing the normal verbal understanding: If the record is altogether intelligible after the fingerprint insertion, this property is accomplished [27], [24] and Robustness: It is the limit of recipient's IDs to survive purposefully, and accidental assaults in the wake of being embedded into the file. On the off chance that the fingerprint is cracked, the estimation of the computerized report is lost [15].

M. Wu et al. have proposed [19] a normal information, concealing structure is starting with an original multimedia (I0), which is otherwise called the cover media (host media), the inserting part embeds in it an arrangement of auxiliary information (b), that is denoted to inserted information or symbol (watermark), to get stamped media (I1). The inserting is finished for instant I1 is relatively coordinating to

I0. The change among of I1 and I0 is damage presented by inserting procedure. Generally, the installed information is a gathering of bits, which can originate from an encrypted form string, since a design, contingent upon the application. The inserted information b will be decoded from the stamped media I1 by as showed in Figure 2.2.

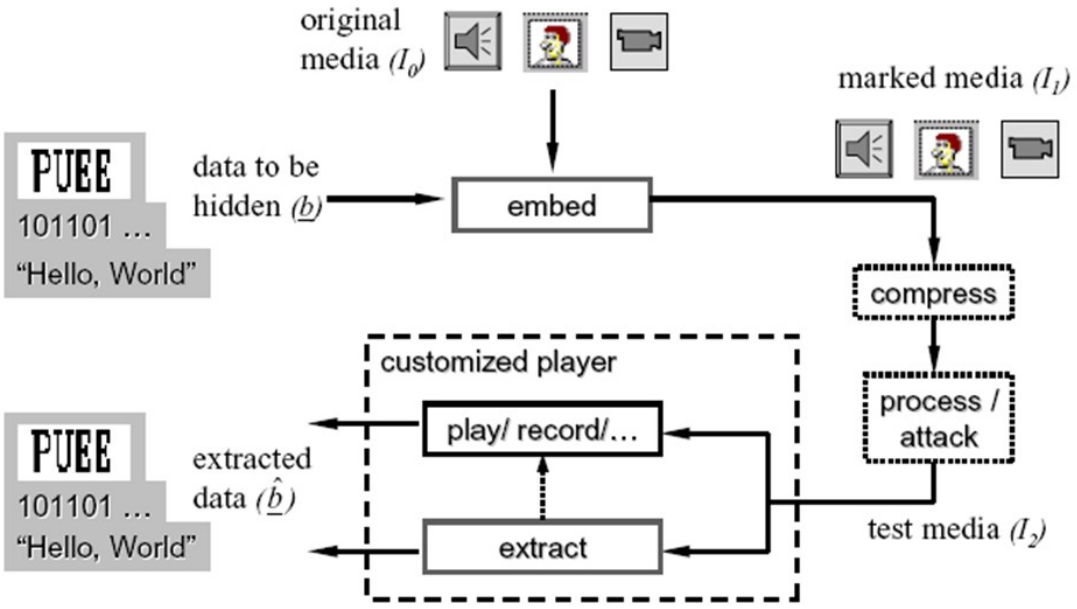


Figure 2.2: General Framework for Data Hiding System.

C. Podilchuk and W. Zeng [3, 2] recommended a watermarking system for computerized images that is taken into account using visual models, which have been created in the setting of image compression. The visual model gives an immediate approach to focus the greatest measure of the watermark sign that every part of an image can endure without influencing the visual nature of the picture. The watermark is encoding pattern comprises of a recurrence decay taking into account a 8 x 8 structure companied by just noticeable difference (JND) estimation and watermark insertion. The watermark method is strong to different assaults, for example, JPEG compression, added multimedia clamor, scaling, and so forth. Additionally clarified the spread spectrum added embedding. [28] Assume host

media is denoted to a vector x, for instance, comprise of the best critical Discrete Cosine Transform (DCT) parts of a image. The proprietor creates watermarks and inserts every element with watermark keen on the host media by y (l) = x(l)+s(l) by y(l), x(l), then s(l) existence the lth segment of the watermarked duplicates, the host media, and the separately watermark. The merits saying in commonsense watermarking, earlier the watermark is additional to the host signal, every part of the watermarks are measured via a suitable component to accomplish the implacability of the installed watermark and additionally regulated the vitality of the inserted watermark. Single plausibility for element is to utilize human visual model with just noticeable difference (JND) [2].

Cox et al proposed spread spectrum methods for insertion have been generally utilized for normal image on the robust that they are powerful for a wide scope of assaults, including agreement collusion assaults [15] the first watermarking system utilizing spread spectrum. In this technique, the beneficiary's fingerprint is symbolized as a spread spectrum series that is presented in the most imperative recurrence locales of the image, subsequent to the less vital territories have a tendency to be dismisses when applying. At the point when the inserted course of action is removed, it is crucial to make a connection with all the known beneficiary arrangements to recognize the fraud. This methodology expands the identification period straightly, and as an afterthought of an agreement assault it considers that all the beneficiaries are liable to conspire, which is not basically rectify. Despite the spread range being utilized as a part of [18] and [1] as an insertion system for computerized multimedia, its imperviousness to agreement collusion assaults has not been stated.

In 2011 [17] an ordered fingerprinting structure in light of Code Division Multiple Access (CDMA). In this structure, beneficiaries are sorted out in gatherings, and the beneficiary's unique fingerprint is indicated by a spread spectrum order, one for the beneficiary ID and another for the gathering ID. These series are orthogonal since they are Discrete Cosine Transform (DCT) premise vectors adjusted by a

pseudo random structure (PN) of 1 and one qualities, permitting maintenance of orthogonality. The spread spectrum series for a crowd i is created by a vector V of length L with all passages equivalent to 0, including a measure of vitality sack to the passage at position i. Sometime recently, the Inverse DCT (IDCT) is utilitarian to V to get the i-th premise capacity of the DCT. At long last, V is adjusted by a grouping PN produced from mystery keys, which offers security to the example in light of the fact that just the person who realizes that the key can recognize crowds. The spread spectrum structure Kuribayashi has proposed wi that is made for the i-th crowd.

## 2.1 Chapter Summary

For somehow, we have seen that some scholars and academicians what have been portrayed about various issues on collusion resistant multimedia fingerprints, and suggested different method to resist collusion attacks. Also shown that there is some consequence facing in their works. By using their different knowledge, it will help make this thesis successful implemented.

# Chapter 3

# Hypothetical Analysis of Fingerprint And Collusion Attacks

This chapter, we take a gander at both the computerized fingerprinting (digital fingerprint) development and the collusion assault procedure together, then may be seen as comprising of three principle parts: fingerprint installing, fingerprint identification, and collusion assaults. At present, let us find at each of these segments independently and watched a few disadvantages of orthogonal fingerprinting and quality (strength) of coded fingerprinting.

## 3.1 Fingerprint Embedding

At the multimedia proprietor's side, for every beneficiary in the framework, he creates an interesting fingerprint of the same degree as the host signal. Because of its strength against numerous assaults by a solitary enemy, Additive spread spectrum inserting [15, 2] is connected to conceal fingerprints in the host sign and human visual models are utilized to ensure the indistinctness of the installed fingerprints. At last, the multimedia proprietor disperses the fingerprinted duplicates to the comparing beneficiaries. Expect that there is a whole of M beneficiaries in the application. Considered a host sign signified by a vector sj of length N, and that wj is the

fingerprint for the ith beneficiary where i = 1, 2. . . M, and it has length N. In orthogonal fingerprint, the M fingerprints are created freely. The fingerprinted duplicate xj that is appropriated to the ith beneficiary is made by X j(i) = S j + $\alpha$j W j( k). As showed in figure 3.1

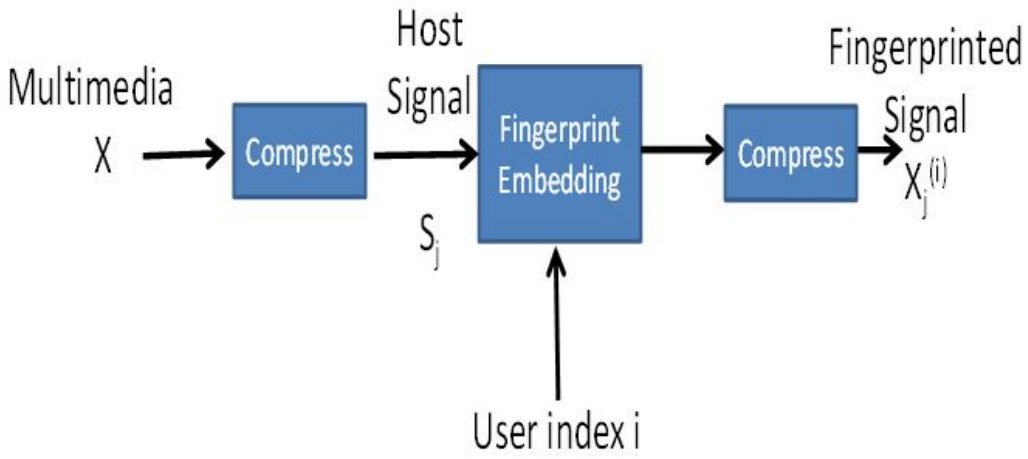


Figure 3.1: Additive Spread-spectrum Embedding.

Where: Xj(i): The fingerprinted duplicate that is conveyed to beneficiary Uj, jth : Components of the fingerprinted duplicate, Sj : The original signal, $\alpha$j : The just-noticeable-difference (JND) from human visual models to control the vitality and accomplish the intangibility of the inserted fingerprints, Wj(i) : The Fingerprint, i: 1,2, ..,M, M: Total beneficiaries,

## 3.2 Fingerprint Detection Process and Colluder Identification

Most imperative in numerous uses of fingerprinting is distinguishing a beneficiary who is redistributing checked multimedia xj by recognizing the fingerprint connected with the beneficiary to whom xj was sold. By recognizing a beneficiary, the

interactive multimedia proprietor may have the capacity to screen future activities of that beneficiary all the more nearly or assemble confirmation supporting that beneficiary's illegal utilization of the multimedia. There are two diverse recognition systems that may emerge in fingerprinting applications. They are separated by the vicinity or unlucky deficiency of the first interactive multimedia in the discovery process.

There is nonblind recognized is the procedure of recognizing the inserted fingerprint with the help of the original multimedia x, Nonblind fingerprint discovery obliges that all the element performing location first recognize the original multimedia adaptation compared to the test image from a database of original multimedia. This database can regularly be extensive and requires impressive capacity assets. In the nonblind fingerprint identification, the mutilation can be demonstrated as n = z. Since a nonblind recognition procedure works at a higher success, and it is best for the colluder identification plan to utilize nonblind location at whatever point conceivable. The nonblind indicator first expels the host signal from the test duplicate before colluder distinguishing proof. At that point, it removes the fingerprint from the test duplicate, measures the comparability between the extricated fingerprint and each of the first fingerprints, contrasts and an edge and yields the assessed personalities of the colluders. x = g({Sk}k$\varepsilon$Sc). Under the nonlinear collusion assaults in the extricated fingerprint is the place g (.) is an arrangement capacity, characterized to testing the vicinity of the multimedia fingerprinted wj in the separated fingerprint

Another blind discovery is the procedure of distinguishing the inserted fingerprinting without the learning of the original multimedia x. Blind discovery plan, on the other side, gives more adaptability component in the discovery procedure, for example, circulated recognition situations. It doesn't require gigantic capacity assets and does not have the computational burden connected with multimedia enlistment from an extensive database. Accordingly especially appealing for empowering fingerprint identification by dispersing confirmation application. Be

that as it may, dissimilar to the nonblind identification situation, in the blind detection situation, the host sign is unidentified to the finder side and regularly goes to as a commotion source that ruins the capacity to recognize the fingerprint. In this circumstance, the distortion can be indicated as n = x + z.as showed in figure 3.2

## 3.3 Collusion Attacks

To watch the relations of nonlinear collusion assaults, the averaging arrangement assault is utilized as the average for the level of the adequacy of collusion. The arrangement of trademark nonlinear collusion that are measured incorporates.

1. Minimum/maximum/median: under these assaults, the colluders make an assaulted sign, in which every part is the Minimum/maximum and median, of the coordinating parts of the fingerprinted signs connected with the colluders.

2. Minmax: every piece of the assaulted sign is the average of the maximum and minimum of the comparing segments of the fingerprinted signs.

3. Modified negative: every piece of the assaulted sign is the contrast between the median and the total of the minimum and maximum of the relating parts of the fingerprinted signs.

4. Randomized negative: every piece of the assaulted sign takes the estimation of the most maximum of the relating parts of the fingerprinted signs with likelihood p and brings the base with likelihood 1 p.

To make it more straightforward to get scientific knowledge, we ordinarily accept that the nonlinear collusion assaults are performed in the same area of highlights as the fingerprint inserting procedure. Further, we take note that it is conceivable to assess the execution for these assaults when the assault space and the inserting area vary by performing trial studies.

Assume that K out of M beneficiaries collude and Sc = {i1 ,i2 , .,ik}is the situated containing the lists of the colluders. The fingerprinted duplicates that are gotten by these K colluders are M{X j (k)}kεSc. The colluders create the jth segment of the assaulted duplicate Vj utilizing one of the accompanying collusion operations:

- Average attack :$V_j^{ave} = \sum_{k\epsilon Sc} \frac{X_j^{(k)}}{K}$
- Minimum attack:$V_j^{Min} = (\{X_j^{(k)}\}_{k\epsilon Sc})$
- Maximum attack:$V_j^{Max} = (\{X_j^{(k)}\}_{k\epsilon Sc})$
- Median attack:$V_j^{Med} = (\{X_j^{(k)}\}_{k\epsilon Sc})$
- Minmax attack:$V_j^{Minmax} = \frac{V_j^{min}+V_j^{max}}{2}$
- Modified negative attack:$V_j^{Modneg} = V_j^{min} + V_j^{max} - V_j^{med}$

The min(X j( k)kεSc), max(X j( k)kεSc), and med (X j( k)kεSc) return the minimum, the maximum, and the median estimations of (X j( k)kεSc), individually. The colluded duplicate is V= {V1, V2,....Vn}. For the fingerprint installing and collusion assault model applying the collusion assaults to the fingerprinted duplicates is reportedly to spread over the agreed assaults to the inserting fingerprints. As shown

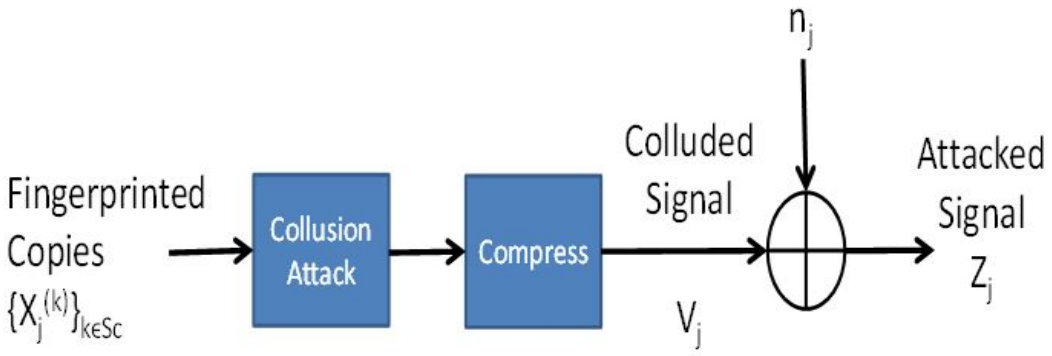


Figure 3.2: Collusion Attack on Fingerprinting.

## 3.4 Orthogonal Fingerprinting Drawbacks

One drawback of orthogonal fingerprints is that its capacity limitation (Small recipients number) by the amount of Orthogonal signal that can be created whereby the quantity of connections orthogonal fingerprint is corresponding to the quantity of beneficiaries or most extreme number of beneficiaries that can be bolstered by an orthogonal fingerprinting is equivalent to the measurement of the orthogonal signs. In numerous interactive media circulation applications, this limitation the measure of recipients that multimedia can be disseminated. Other conceivable downside with orthogonal regulation is the high computational many-sided quality needed for location connected with assessing which beneficiaries of multimedia is available when the aggregate number of beneficiaries is substantial this prompts noteworthy discovery multifaceted nature in light of the fact that this number of relationships is equivalent to the quantity of recipients .This is on account of the standard technique for identification engagements an arrangement of coordinated channels that relate the test sign against every fingerprint.

Following drawback of orthogonal fingerprints is large storage required need to maintain a library of fingerprints whereby fingerprint detection obliges a system for perceiving the multimedia from a database, which can frequently require impressive capacity assets so in this orthogonal fingerprints suit extensive capacity in applications. Disadvantage of orthogonal fingerprints as well as by installing one of a kind fingerprints in different duplicates of multimedia which is a commonly orthogonal sign is distributed to every beneficiary as a unique fingerprint to concur the multimedia proprietor or to follow colluders who made unlawful duplicates, the same number of relationship as the quantity of beneficiaries is obliged so that the identification, that when the quantity of multimedia included in the averaging assault builds, the quality of orthogonal signs is debilitated legitimately so that the locator can't effectively follow colluders.

Moreover significant drawback of orthogonal fingerprinting is energy reduction of the fingerprints sign amid arrangement assaults; the fingerprinting utilizing

orthogonal balance is its extreme vitality decrease. For example, under the averaging collusion, the subsequent vitality of the connived duplicate is lessened to 1/K of the multimedia fingerprint vitality, with K presence the quantity of colluders. This energy reduction essentially corrupts the recognition presentation of every unique fingerprint. The relationship concern additionally serves to lessening the vitality decrease proportion saw on account of orthogonal regulation. Additionally incorporated, the drawback of orthogonal fingerprints utilized non-blind identification is the procedure of identifying the installed interactive media with the help of the original multimedia, non-blind fingerprint discovery gives high trust in recognition.

## 3.5 Coded Fingerprinting Strength

One strength coded fingerprints was designed to support many number of recipients for constructing non orthogonal fingerprints becomes necessary. In such that to supporting a larger number of fingerprints than the dimensionality of the highlight sign or preventive the quantity of orthogonal premise signals for lessening reckoning intricacy. By utilizing orthogonal fingerprinting is excessively prohibitive, therefore, attractive to search for other fingerprinting systems that coded fingerprinting can bolster a bigger client base, while likewise having the capacity to oppose the collusion. Further, another significant quality of coded fingerprints obliged less stockpiling assets considers appropriated discovery situations it doesn't require huge capacity assets or have expansive computational expenses connected with multimedia registration.

Another strength of coded fingerprints is inserting diverse fingerprints in numerous duplicates of multimedia, for that methodology was acquainted connections into distinctive fingerprints with permit exact recognizable proof of the contributing fingerprints included in collusion. This encourages multimedia for drawing in conveyed assets, wherever the finders are liable to have confined

computational capabilities, it is significant to chop down the amount of connections utilized. In extra to coded fingerprints quality is utilized Blind discovery; the procedure of recognizing the installed multimedia without the information of the original multimedia, that it settled the unpredictability of recognition can be a sympathy toward orthogonal fingerprints amid identification must be original multimedia present and enhanced the computational effectiveness of discovery for an orthogonal fingerprinting. On other hand coded fingerprints strength are suitable for both average collusion assaults and linear, whereby developing fingerprints that obliged little stockpiling assets so that interleave estimations of pixels from distinctively checked adaptations of several multimedia of the same multimedia this is higher avoidance against those assaults specified.

## 3.6 Chapter Summary

In this chapter, we have given the hypothetical examination itemizing the viability of diverse collusion assaults against multimedia fingerprints. We considered the perceptual nature of the assaulted signal under distinctive collusion assaults. We likewise explored a few regularly utilized identification mechanism under these collusion attacks and fingerprint embedded process. Also, we have seen the multimedia fingerprinting components strength and drawbacks of the two fingerprinted resistant algorithms.

# Chapter 4

# Proposed Implementation Fingerprinting Model

In this chapter, we look the experimental implementation of the coded fingerprint process where fingerprint embedding and fingerprint extraction. Due to some observation of the drawbacks of orthogonal fingerprinting like; energy reduction of the fingerprints signal during collusion attacks and capacity limitation, so we have proposed to implement coded fingerprinting where by having a lot of strengths to the collusion attack process and able to resist for somehow. Now let us discover the attached components of the fingerprinting system to embed multimedia file and extraction of those components to trace colluders. First, let us look the coded fingerprinting model as displayed in figure 4.1 below.

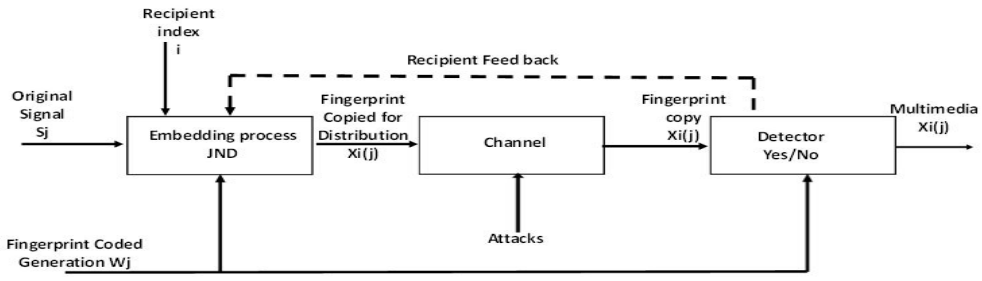


Figure 4.1: Components of the Coded Fingerprinting Process.

## 4.1 Algorithm for Program

*Algorithm* :

1. Insert multimedia content to the program Sj;
2. Coded fingerprint is generated for recipients Wj;
3. Embedding coded fingerprint inform of just noticeable difference (JND);
4. Assigned to the recipients i;
   If (the multimedia fingerprint generated and embedded)
   fingerprint copied distributed;
   else
   back to Step 1;
5. Fingerprint copied, transmitted to recipients k;
6. Recipient made correlation between fingerprint copy and coded fingerprint;
   If (fingerprint copy = = code fingerprint)
   multimedia content extract;
   else
   Message "Unauthoried User";

## 4.2 Experimental Program

The designing and testing for an application to embed and extract information in using coded fingerprinting technique. The multimedia embedding technique in this program is based on embedding algorithm above. The program was put into two experiments that are information embedding and information extracting or encoder (embedded) side and decoder (Extraction) side. This is a Web application. The application was developed in PHP, Java Script, HTML, and CSS. It is compatible with all types of web server and can access to any kind of browser like Internet

Explorer, Opera, Firefox, Safari etc. The system is both an online application and LAN, if an online can be accessed anywhere as long as having Internet access. A Graphical User Interface was to be created simply because to attract users and it is easy to use without much knowledge of using computer.

## 4.3 Features Supported by the Application

- Digital fingerprint embedding of an image using algorithm mentioned. It can be used as a web application system.
- Embed for individual Authorized to encrypt an image file in the form of just noticeable different (JND).
- Decryption an image file (Extraction), It used blind detection, thus without original image exist, Only Authorizes recipient can access the image.
- Different fingerprint is embedded into the different copy of an image, so collude will not able to identify the fingerprinted embedded that is resistant against collusion attacks multimedia fingerprint.
- Fingerprinted images saved or stored in the same format as the original images.

## 4.4 How the Application Work

The window of the system which shows the embed or encryption graphic interface as shown in the figure 4.2 below

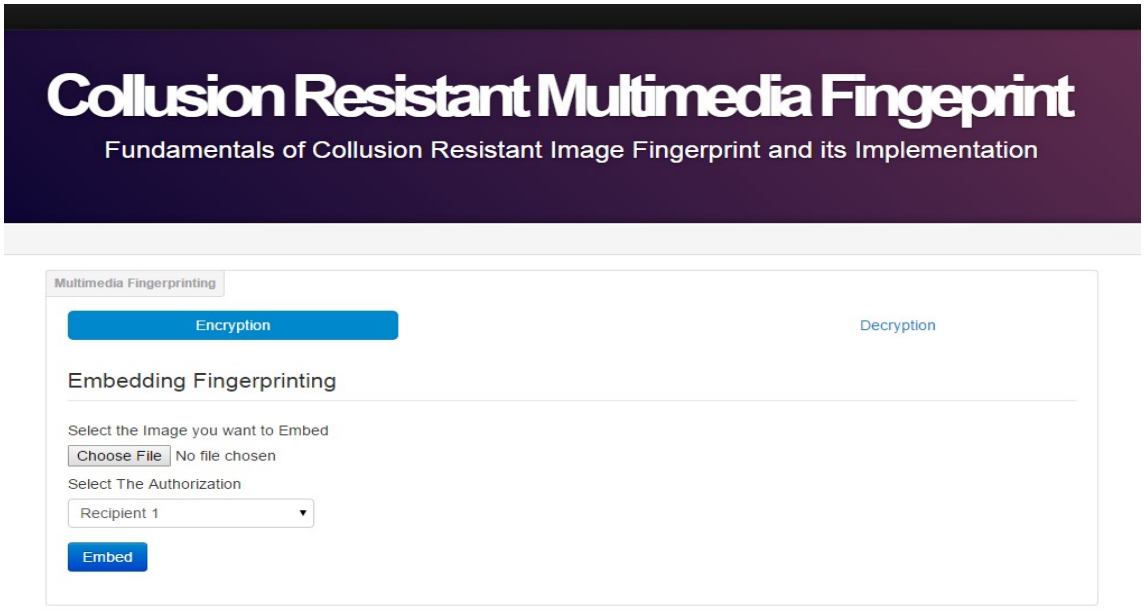


Figure 4.2: Views Encryption Graphic Interface Window for Application.

The window of the system which shows the extraction or the decryption graphic interface as shown in the figure 4.3 below

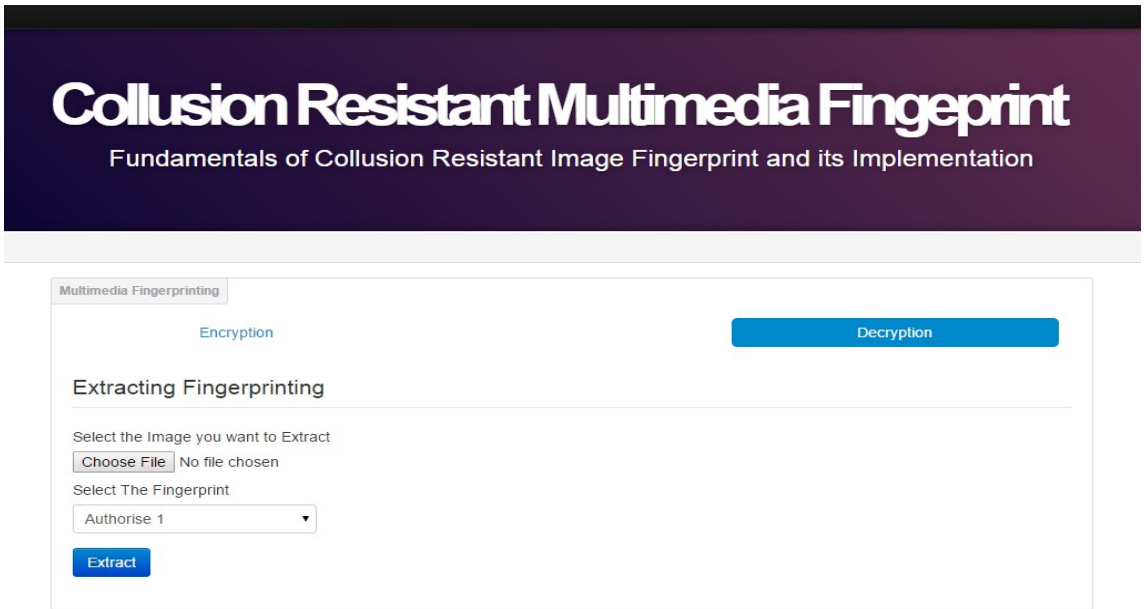


Figure 4.3: Views Decryption Graphic Interface Window for Application.

### 4.4.1 Embedding Process

Embedding process starting for choose file button to find multimedia file where it was saved and captured it and insert into a program as shown in figure 4.4 below

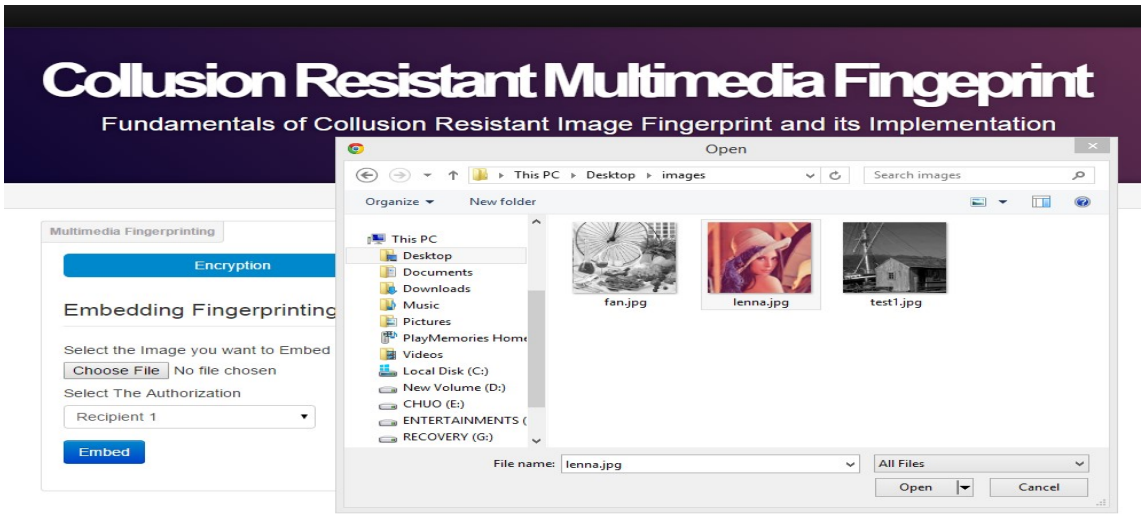


Figure 4.4: Selecting Fingerprint to Embed.

Select the fingerprint to embed into multimedia components by selecting recipient, you wish to send the multimedia as shown in figure 4.5 below

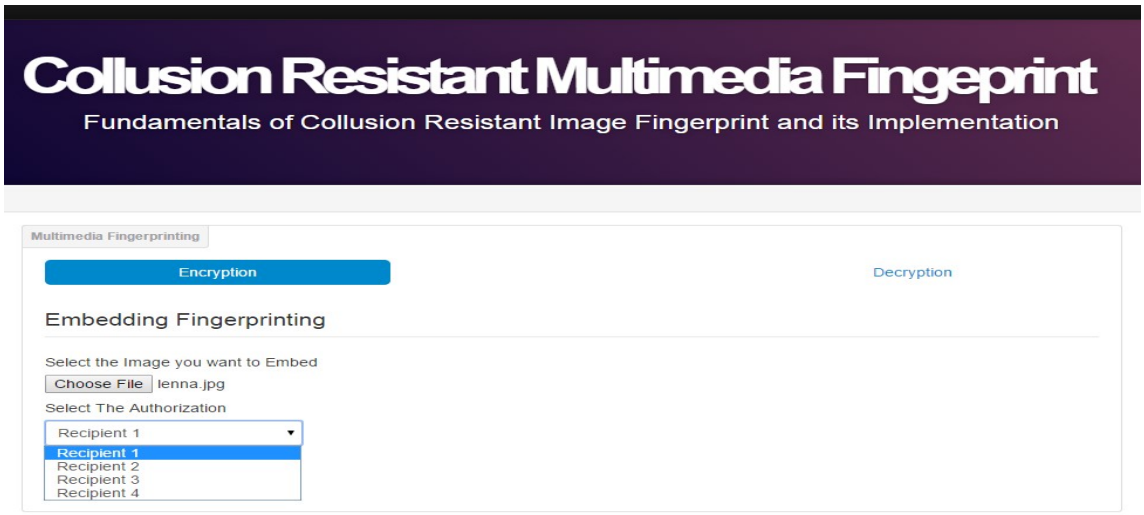


Figure 4.5: Selecting Fingerprint to Embed.

Embedding process continue by capturing image and selecting fingerprint then press button Embed to encrypt the multimedia (encode the information) as shown in figure 4.6 below

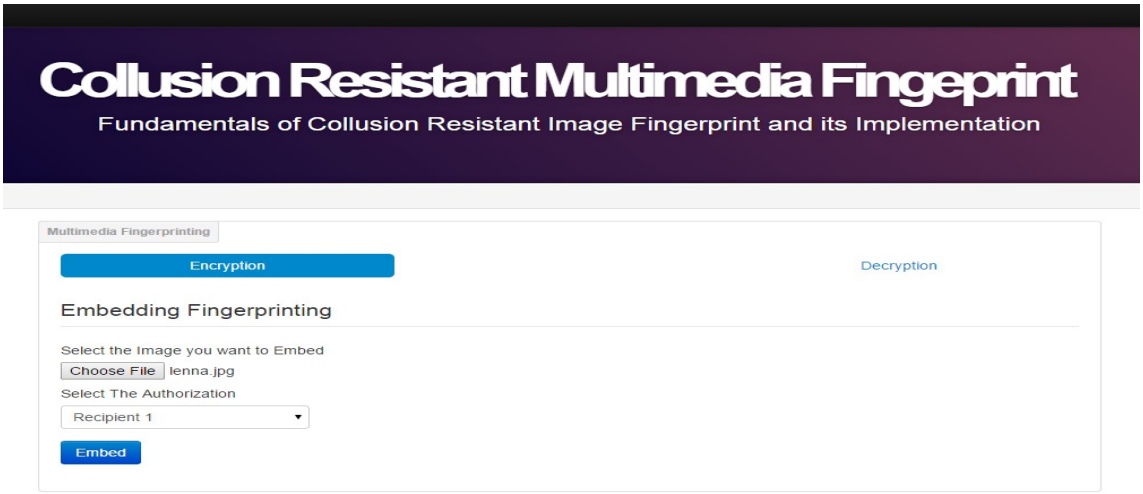


Figure 4.6: Embedding Process.

The embedded process completed in order to save it your image you have to press download button to save your image as shown in figure 4.7 below

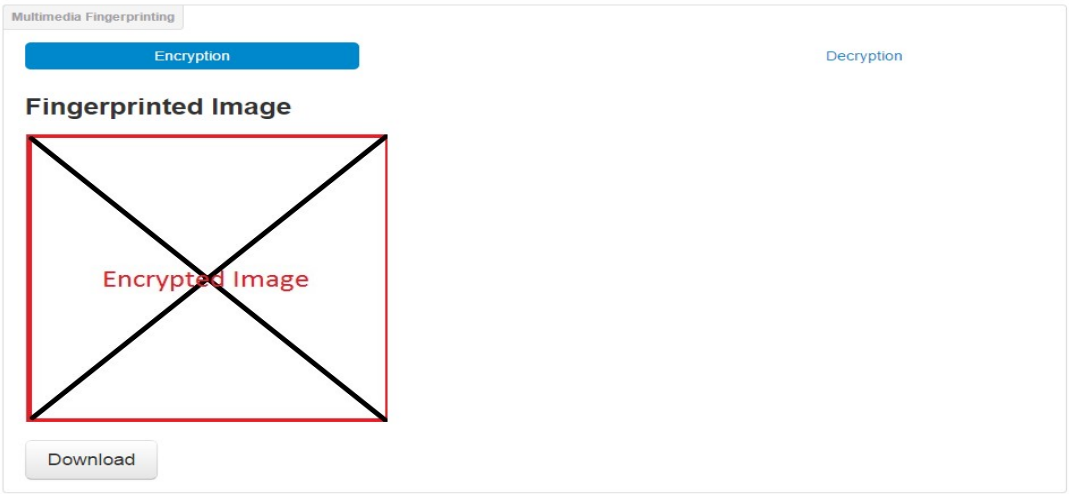


Figure 4.7: Information Embedding Fingerprint Components.

Pop menu display confirmation if you want to save or not the embedded multimedia by click save image as shown in figure 4.8 below

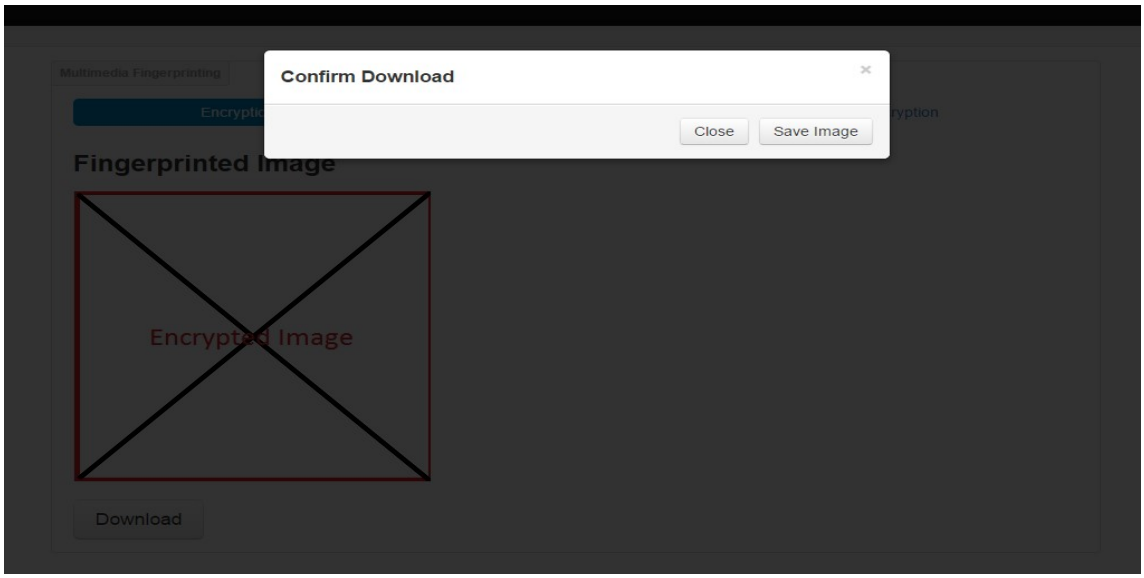


Figure 4.8: Confirmation Download.

After confirmation done file starting downloading as shown in figure 4.9 below

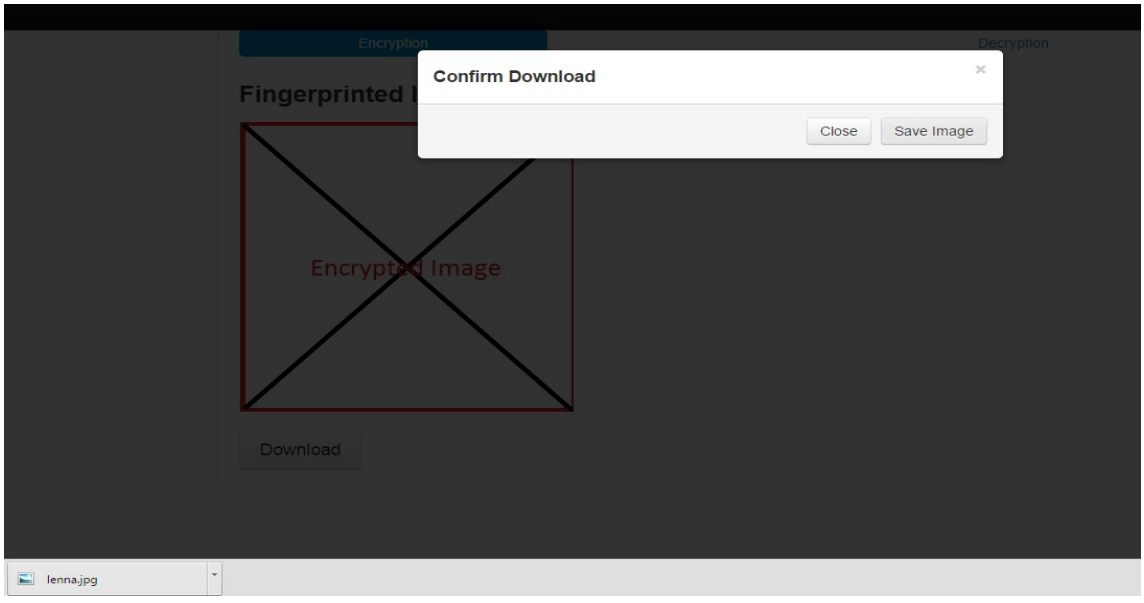


Figure 4.9: Download Process.

This is the encrypt image save into the download folder in the computer or where the browser allocates as shown in figure 4.10 below

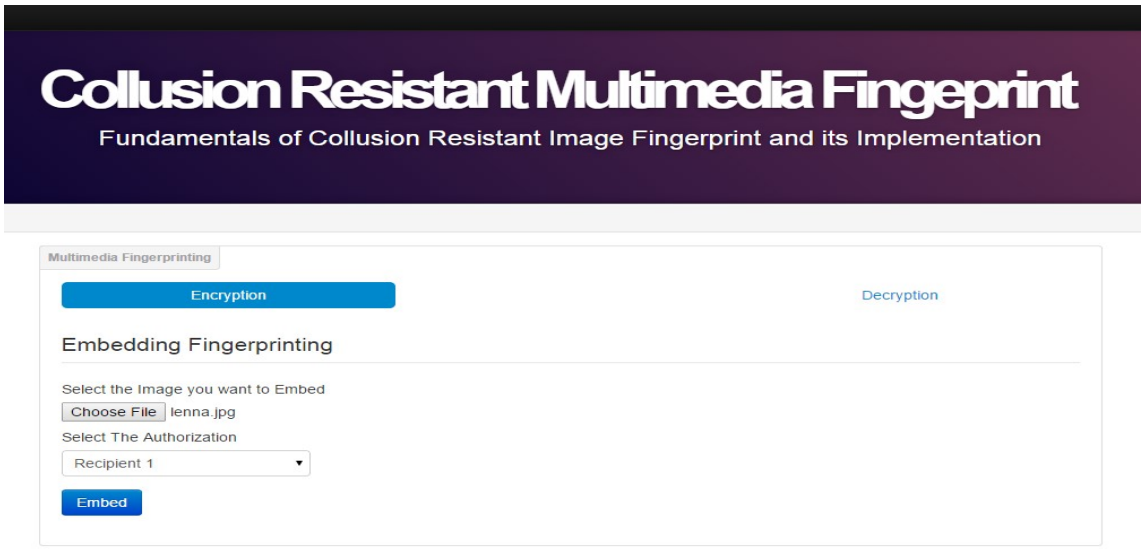


Figure 4.10: Saved File.

The display, encrypt image or fingerprinted image in downloads folder as shown in figure 4.11 below

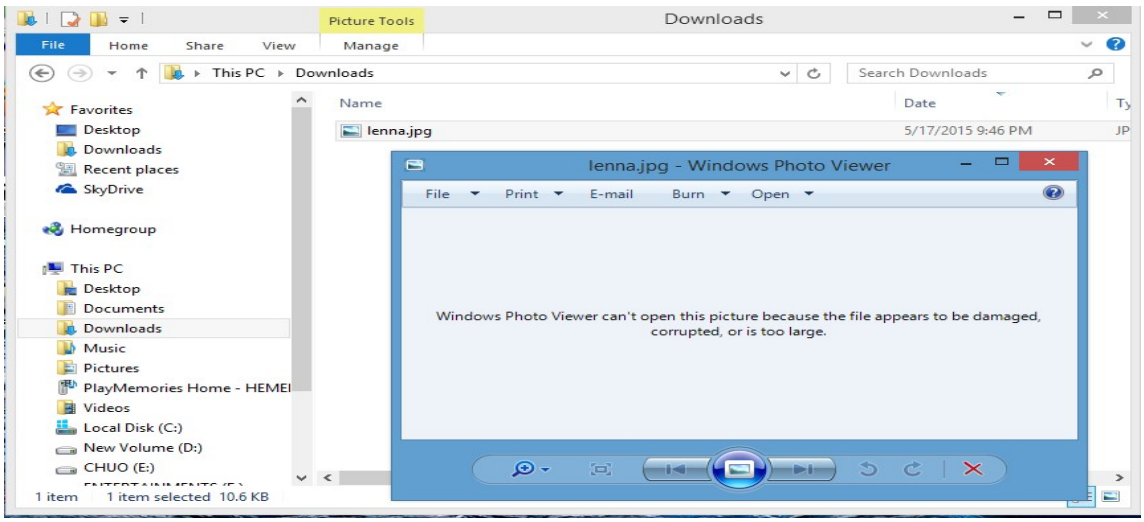


Figure 4.11: Fingerprinted Image.

### 4.4.2 Extraction Process

Decryption process starting by choose file button to find multimedia file where it was saved and captured it and inserted into a program as shown in figure 4.12 below

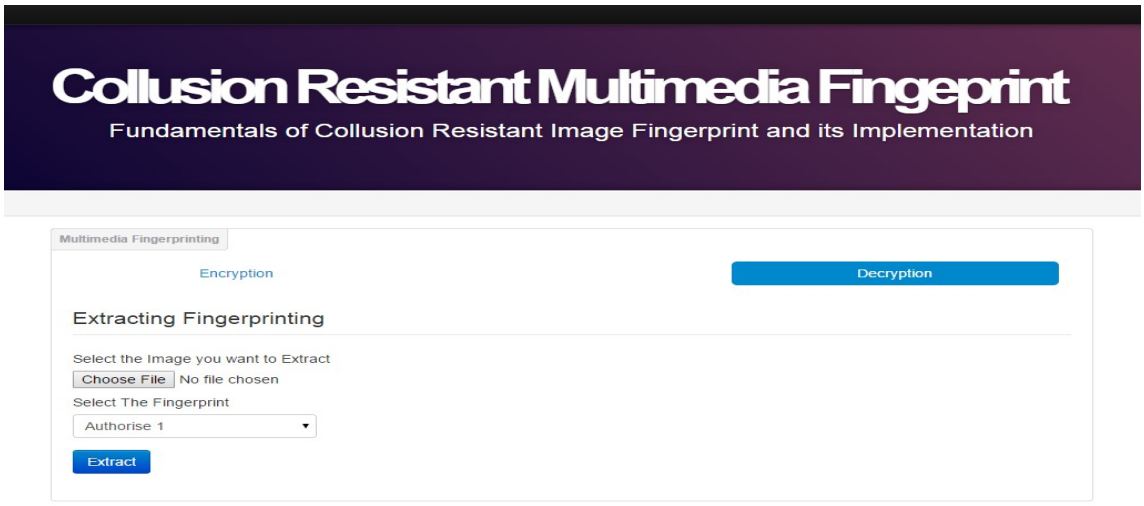


Figure 4.12: Open Encrypted Image.

Choose file button to find multimedia file you want to decrypt and select image and insert into a program as shown in figure 4.13 below

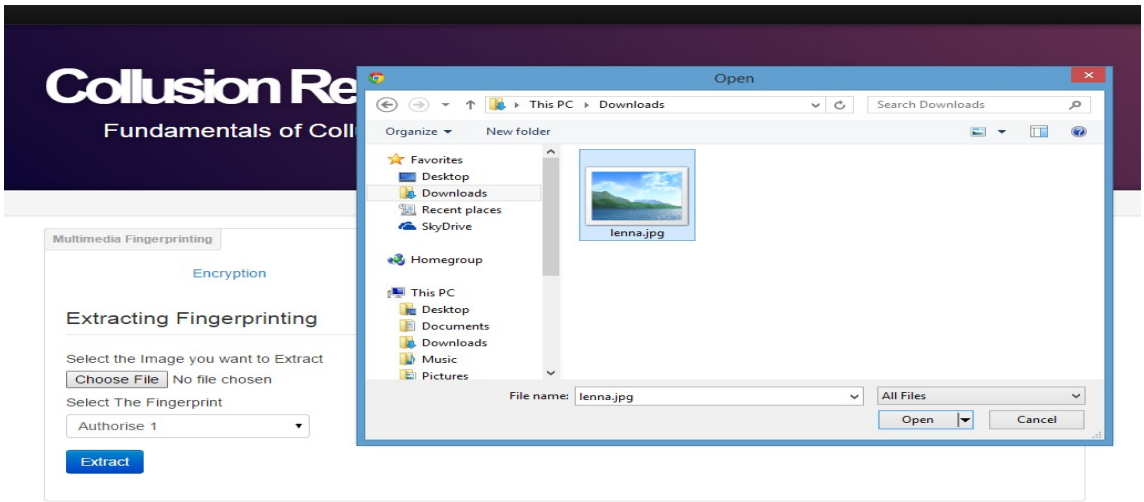


Figure 4.13: Encrypted Image.

The image selected and captured by the application as shown in the figure 4.14 below

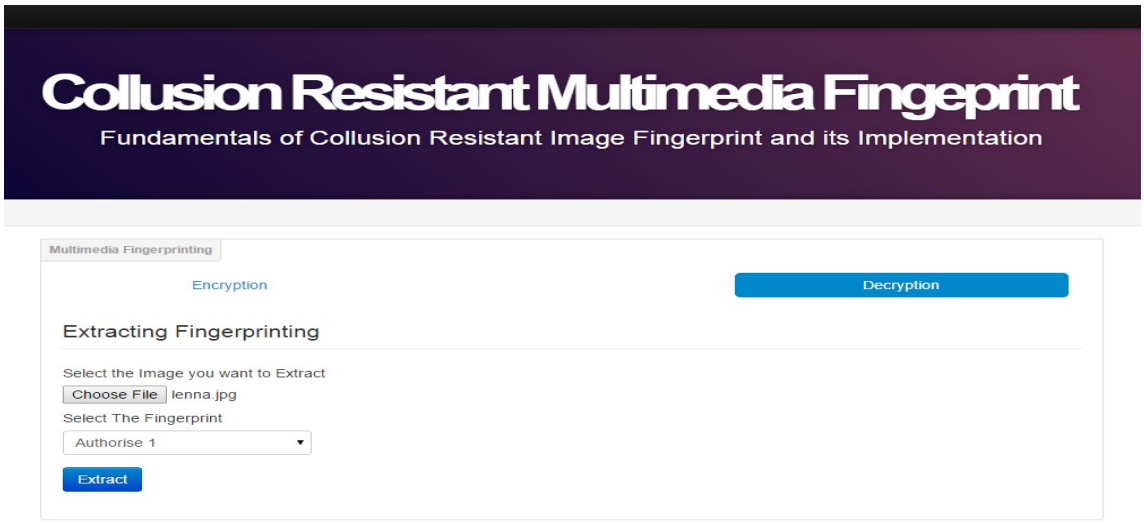


Figure 4.14: Capture File for Extraction.

Select the authorized to extract to the multimedia components by selecting his authorization fingerprint which one sends for him to open the multimedia content as shown in figure 4.15 below

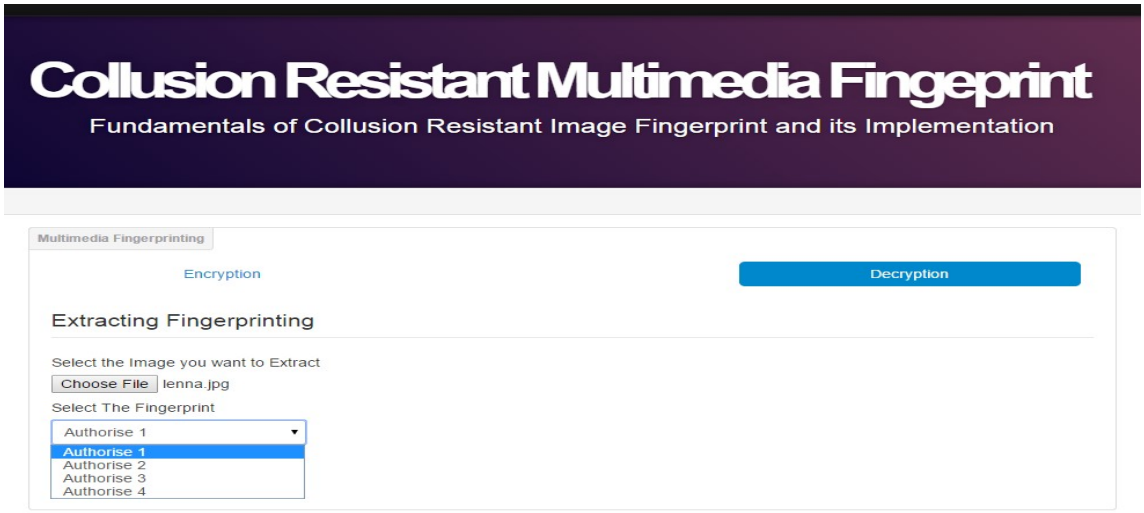


Figure 4.15: Select Authorization to Extract Image File.

The application is extracted Information of the fingerprints components from the multimedia file and decode the information by capture encrypted image and select authorization fingerprint then press Extract button to decrypt the multimedia contents as shown in figure 4.16 below

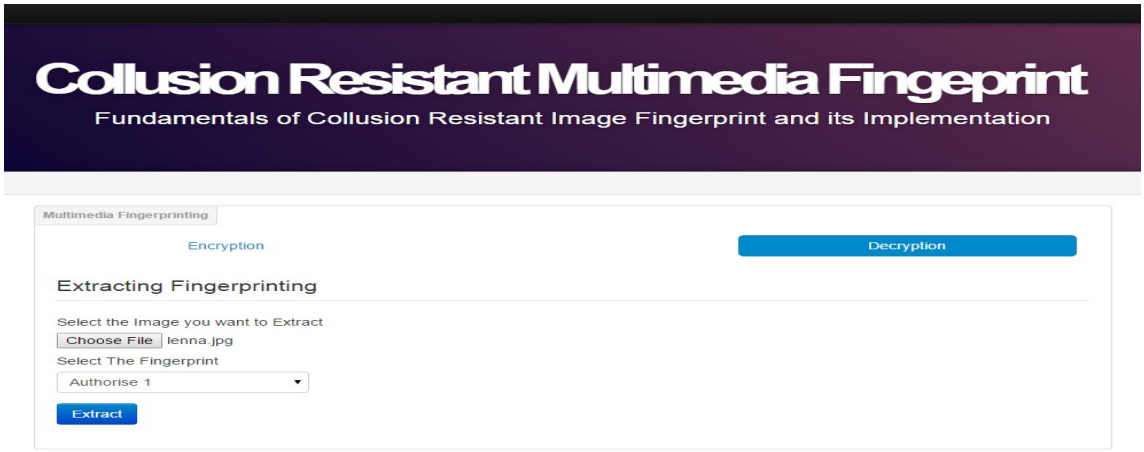


Figure 4.16: Extraction Process.

The program is extracting or decode Information of the fingerprints components from the multimedia file. The extraction process completed in order to save it your image you have to press download button to save your original image as shown in the figure 4.17 below

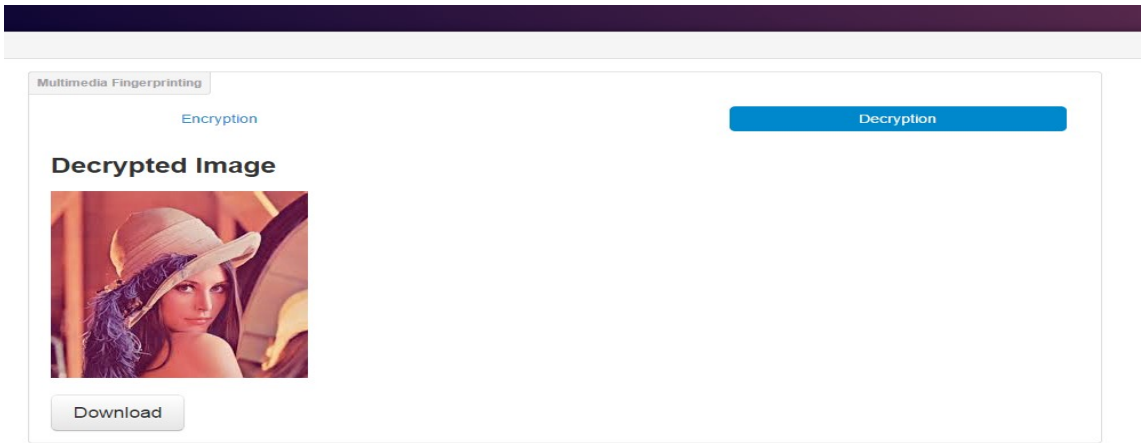


Figure 4.17: Extraction Fingerprint Image.

Pop menu displays to confirm if you want to save or not the extraction component by click save image as shown in the figure 4.18 below

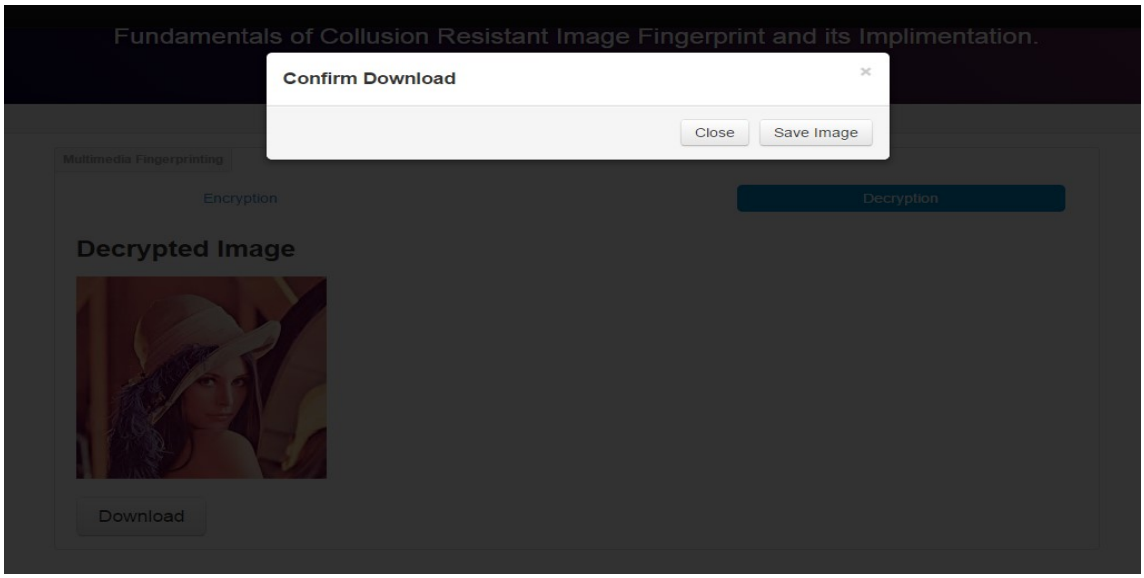


Figure 4.18: Confirmation File Download.

After confirmation done downloading has started as shown in the figure 4.19 below

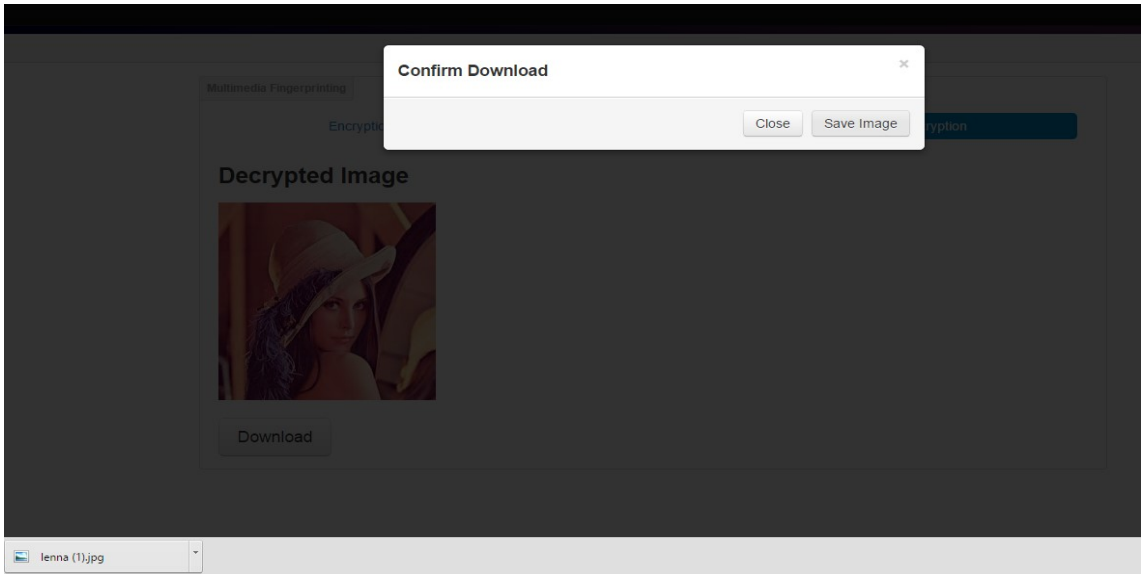


Figure 4.19: Download Process.

The displayed decrypt image or original image as shown in the figure 4.20 below

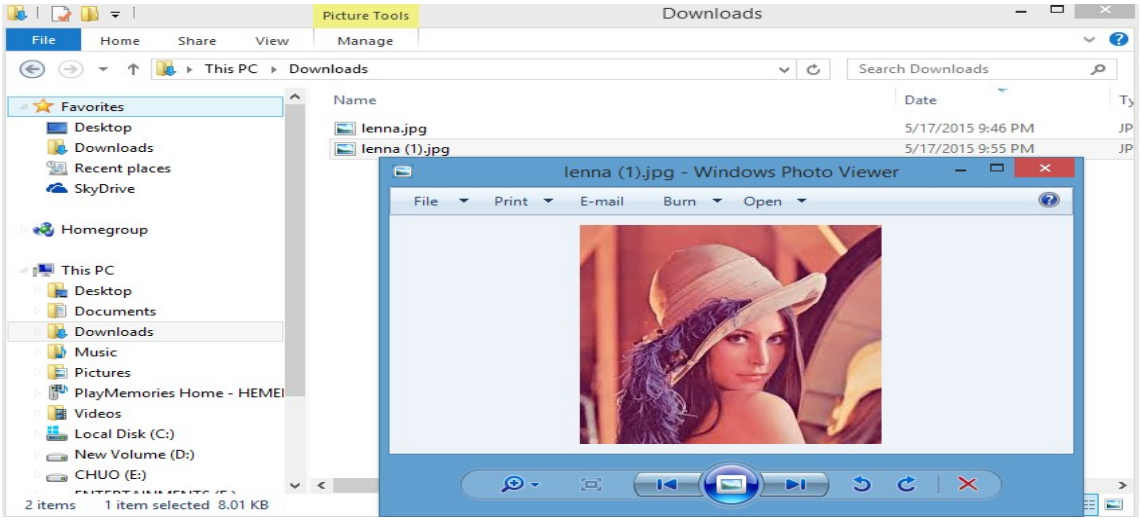


Figure 4.20: Extraction File.

### 4.4.3 Collusion Tries

This Interface displays when anyone tries to decrypt image or extract fingerprinted image that is not authorized by the owner as shown in figure 4.21 below

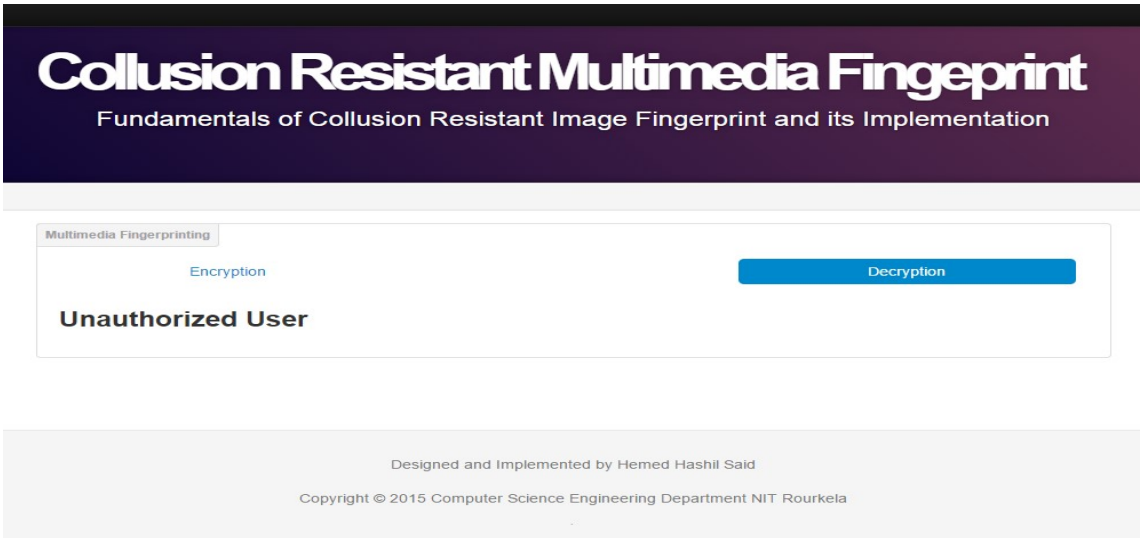


Figure 4.21: Unauthorized User.

### 4.4.4 Collusion Resistant Results

The results of the all process of Embedding and Extracting Experiments We showed an embedding and extracting experiments using a web application. Our major concerns are embedding multimedia and extracting multimedia as shown in the figure 4.22 below

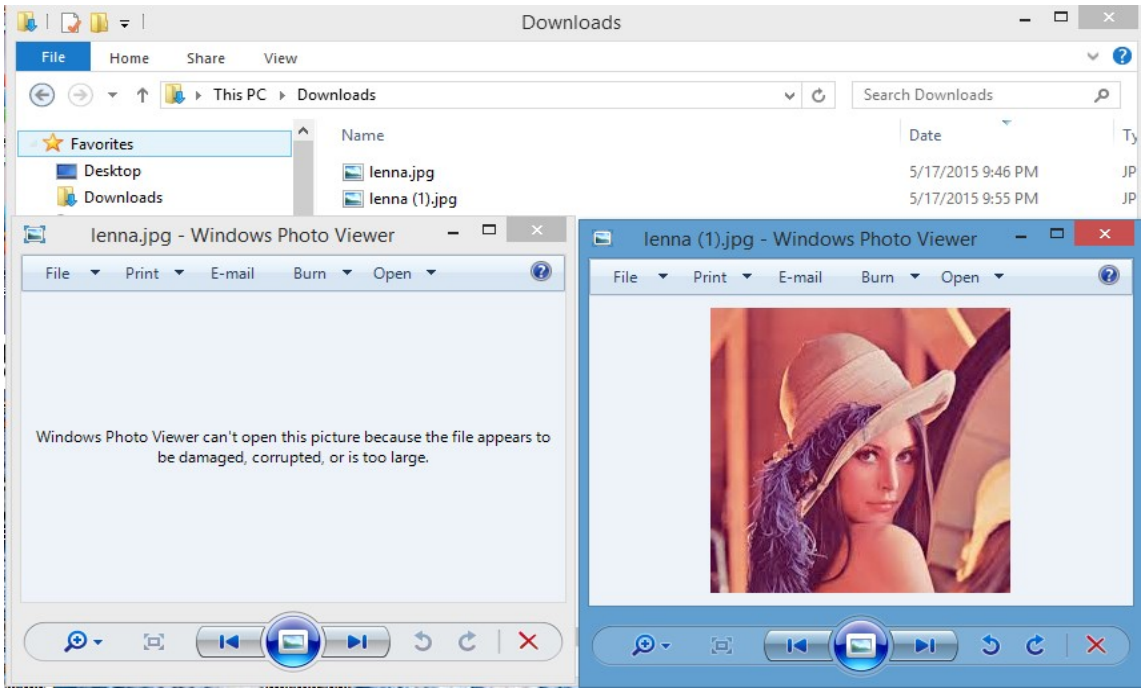


Figure 4.22: Results of Embedding and Extracting Experiments.

When the recipients extracting the multimedia the owner of the multimedia received email to his or her mail sat in the system to alert or provide feedback to the multimedia Owner either correct fingerprinted used or collision attack tries to extract the multimedia figure 4.23 below

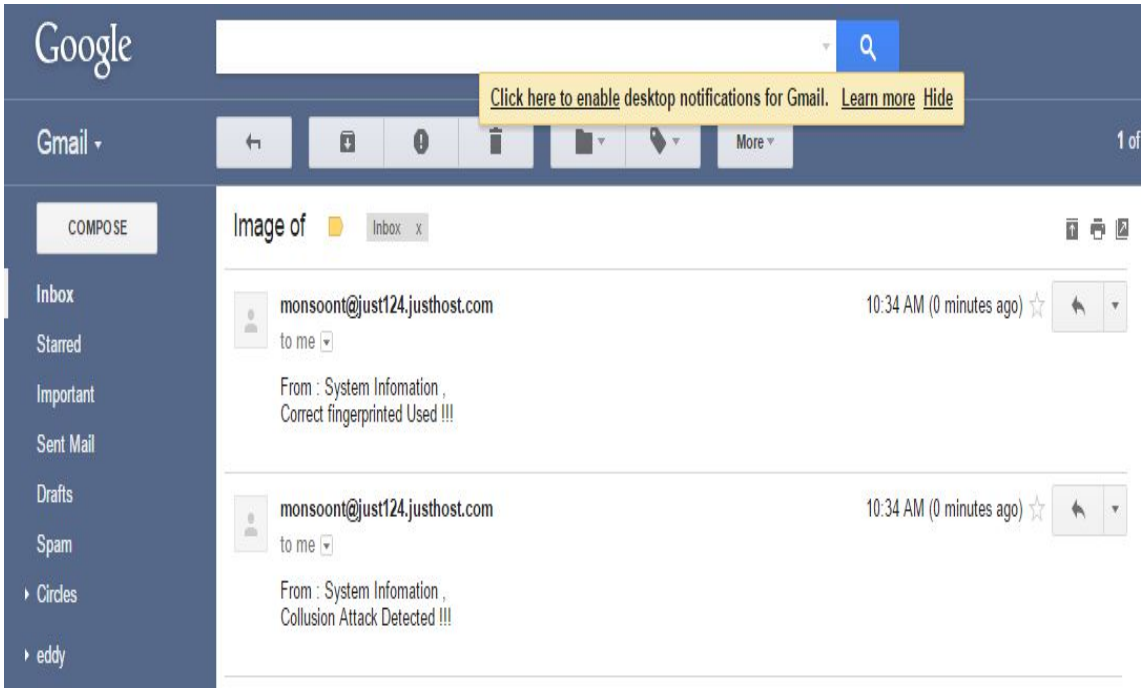


Figure 4.23: Mails to the Owner.

## 4.5 Chapter Summary

We have seen the proposed implementation coded fingerprinting model, algorithm and experimental application that was designed for embedding and extracting multimedia. And also seen how that program performed their task to provide the desired output for protecting multimedia content against unauthorized recipients (collusion attacks).

# Chapter 5

# Conclusion And Future Work

## 5.1 Conclusion

In this thesis, we have examined two schemes, tactics for multimedia protection using content encryption and embedded fingerprints. Content encryption fingerprints can be used to prevent the redistribution of multimedia through the channel while embedded fingerprints can be used to trace individual copies and detector recipients from unauthorized redistribution. We had successfully embedded a fingerprinting in an image that is used for owner identification, and we had effectively actualized the fingerprinting framework that can oppose the agreement assaults and follow colluders.

We surveyed theoretically and empirically in the existing algorithms on collusion resistant multimedia fingerprints and came up with the application that can resist the collusion attacks. Each fingerprint is studied to understand its influence on the identification accuracy or correct recipients. The blind detection mechanism is the procedure of recognizing the inserted media lacking of information about original multimedia. The blind discovery considers circulated identification situations it doesn't require endless capacity assets or have important computational expenses connected with substance recording.

In additional we analyzed the attacks on multimedia fingerprint simply by synchronizing the signals of media and average the signal, which is an occurrence of the linear collusion assault (average assault). Other collusion assault, indicated to as the copy and paste assault that includes beneficiaries removing parts of each of their media flags and gluing them together to frame another variant of the sign. Different assaults can utilize nonlinear operations, for example, taking the most median or maximum of the benefits in relating parts of each duplicates.

Not only it is user friend, but also interactive application was designed. The collusion resistant application has attractive interfaces that are easy to use. After the application had been developed, it was tested to ensure that it was functioning as expected to ensure higher security in multimedia collusion attacks. Also the collusion resistant application will ensure to protect multimedia from unauthorized distribution, It increased efficiency and effectiveness in protecting multimedia content and permit only authorized recipients to access multimedia content, This achieved by use of an individual fingerprint attached with multimedia file.

## 5.2 Future Work

Followings are future scope of this research work: Examining resistance against other collusion attacks and improved fingerprinting using additive spread-spectrum techniques. Because of the development of the internet utilization, there are several new sorts of collusion attacks that may carried out against fingerprinting algorithms. Such attacks pose a critical risk to fingerprinting multimedia. To reveal the hidden complexities administering the impact of those assaults, both systematic and trial studies on their conduct need to be done further.

Designing multimedia distribution protocols over networks is another future direction. The appearance of electronic trade and the making of electronic dissemination channels for media substance have new difficulties in regards to the security of protected innovation. That is, to secure the welfare and hobbies of

the multimedia proprietor, or supplier, it is not kidding to guarantee the suitable appropriation and approved use of an interactive media content. The fingerprinting technique alone is not sufficient and should be used together with other information protection technologies. In addition to the secure and efficient transmission of multimedia content and traitor tracing requirement, user authentication and personal information protection should also be considered in the distribution protocols.

# Bibliography


[1] Bin He, Yuqian Wu, Kai Kang, and Wei Guo. A robust binary text digital watermarking algorithm for print-scan process. In *Computer Science and Information Engineering, 2009 WRI World Congress on*, volume 7, pages 290–294. IEEE, 2009.

[2] Christine I Podilchuk and Wenjun Zeng. Image-adaptive watermarking using visual models. *Selected Areas in Communications, IEEE Journal on*, 16(4):525–539, 1998.

[3] Christine Podilchuk and Wenjun Zeng. Perceptual watermarking of still images. In *Multimedia Signal Processing, 1997., IEEE First Workshop on*, pages 363–368. IEEE, 1997.

[4] Dan Boneh and James Shaw. Collusion-secure fingerprinting for digital data. *Information Theory, IEEE Transactions on*, 44(5):1897–1905, 1998.

[5] Deepa Kundur and Kannan Karthik. Video fingerprinting and encryption principles for digital rights management. *Proceedings of the IEEE*, 92(6):918–932, 2004.

[6] Jose Juan Garcia-Hernandez, Claudia Feregrino-Uribe, and Rene Cumplido. Collusion-resistant audio fingerprinting system in the modulated complex lapped transform domain. *PloS one*, 8(6):e65985, 2013.

[7] John G Proakis. *Intersymbol Interference in Digital Communication Systems*. Wiley Online Library, 2001.

[8] Jonathan K Su, Joachim J Eggers, and Bernd Girod. Capacity of digital watermarks subjected to an optimal collusion attack. In *European Signal Processing Conference (EUSIPCO 2000)*. Citeseer, 2000.

[9] Joe Kilian, F Thomson Leighton, Lesley R Matheson, Talal G Shamoon, Robert E Tarjan, and Francis Zane. Resistance of digital watermarks to collusive attacks. In *IEEE International Symposium on Information Theory*, pages 271–271. INSTITUTE OF ELECTRICAL ENGINEERS INC (IEEE), 1998.

[10] Jack T Brassil, Steven Low, Nicholas F. Maxemchuk, and Lawrence O'Gorman. Electronic marking and identification techniques to discourage document copying. *Selected Areas in Communications, IEEE Journal on*, 13(8):1495–1504, 1995.

[11] KJ Ray Liu. *Multimedia fingerprinting forensics for traitor tracing*, volume 4. Hindawi Publishing Corporation, 2005.

[12] Shuhui Hou. Anti-collusion fingerprinting for multimedia content protection. 2009.

[13] H Vicky Zhao, Min Wu, J Wang, and KJ Ray Liu. Forensic analysis of nonlinear collusion attacks for multimedia fingerprinting. *Image Processing, IEEE Transactions on*, 14(5):646–661, 2005.

[14] Hong Zhao, Min Wu, Z Jane Wang, and KJ Ray Liu. Nonlinear collusion attacks on independent fingerprints for multimedia. In *Acoustics, Speech, and Signal Processing, 2003. Proceedings.(ICASSP'03). 2003 IEEE International Conference on*, volume 5, pages V–664. IEEE, 2003.

[15] Ingemar J Cox, Joe Kilian, F Thomson Leighton, and Talal Shamoon. Secure spread spectrum watermarking for multimedia. *Image Processing, IEEE Transactions on*, 6(12):1673–1687, 1997.

[16] Ingemar J Cox, Joe Kilian, Tom Leighton, and Talal Shamoon. Secure spread spectrum watermarking for images, audio and video. In *Image Processing, 1996. Proceedings., International Conference on*, volume 3, pages 243–246. IEEE, 1996.

[17] Minoru Kuribayashi. Hierarchical spread spectrum fingerprinting scheme based on the cdma technique. *EURASIP Journal on Information Security*, 2011(1):502782, 2011.

[18] Muhammad Abdul Qadir and Ishtiaq Ahmad. Digital text watermarking: secure content delivery and data hiding in digital documents. *Aerospace and Electronic Systems Magazine, IEEE*, 21(11):18–21, 2006.

[19] Min Wu and Bede Liu. *Multimedia data hiding*. Springer Science & Business Media, 2003.

[20] Rainer Schick and Christoph Ruland. Document tracking-on the way to a new security service. In *Network and Information Systems Security (SAR-SSI), 2011 Conference on*, pages 1–5. IEEE, 2011.

[21] Shiguo Lian, Dimitris Kanellopoulos, and Giancarlo Ruffo. Recent advances in multimedia information system security. *Informatica (Slovenia)*, 33(1):3–24, 2009.

[22] Steven H Low, Nicholas F Maxemchuk, and Aleta M Lapone. Document identification for copyright protection using centroid detection. *Communications, IEEE Transactions on*, 46(3):372–383, 1998.

[23] Wade Trappe, Min Wu, and KJ Ray Liu. Collusion-resistant fingerprinting for multimedia. In *Acoustics, Speech, and Signal Processing (ICASSP), 2002 IEEE International Conference on*, volume 4, pages IV–3309. IEEE, 2002.

[24] Xinmin Zhou, Zhicheng Wang, Weidong Zhao, Sichun Wang, and Jianping Yu. Performance analysis and evaluation of text watermarking. In *Computer Network and Multimedia Technology, 2009. CNMT 2009. International Symposium on*, pages 1–4. IEEE, 2009.

[25] Xinmin Zhou, Weidong Zhao, Zhicheng Wang, and Li Pan. Security theory and attack analysis for text watermarking. In *E-Business and Information System Security, 2009. EBISS'09. International Conference on*, pages 1–6. IEEE, 2009.

[26] Yongdong Wu. Linear combination collusion attack and its application on an anti-collusion fingerprinting. In *ICASSP (2)*, pages 13–16, 2005.

[27] Zunera Jalil and Anwar M Mirza. A review of digital watermarking techniques for text documents. In *Information and Multimedia Technology, 2009. ICIMT'09. International Conference on*, pages 230–234. IEEE, 2009.

[28] Z Jane Wang, Min Wu, Wade Trappe, and KJ Ray Liu. Group-oriented fingerprinting for multimedia forensics. *EURASIP Journal on Applied Signal Processing*, 2004:2153–2173, 2004.